United States
Environmental Protection
Agency

Response Protocol Toolbox: Planning for and Responding to Drinking Water Contamination Threats and Incidents

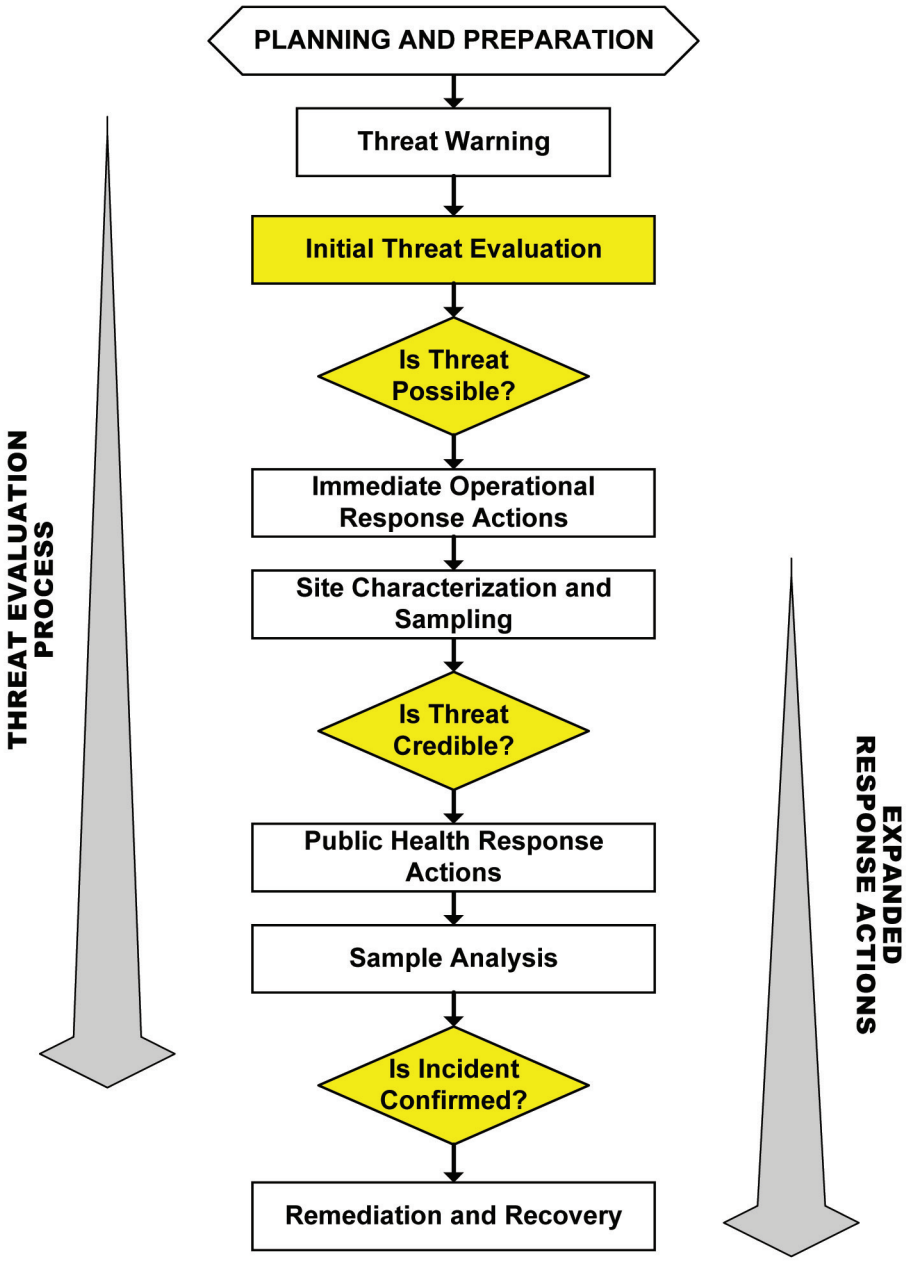
Interim Final - December 2003

Module 2: Contamination Threat Management Guide

Response Protocol Toolbox:
Planning for and Responding to
Drinking Water Contamination Threats and Incidents

Module 2: Contamination Threat Management Guide

Interm Final - December 2003



OTHER RESPONSE PROTOCOL TOOLBOX MODULES

Module 1: Water Utility Planning Guide *(December 2003)*
Module 1 provides a brief discussion of the nature of the contamination threat to the public water supply. The module also describes the planning activities that a utility may undertake to prepare for response to contamination threats and incidents.

Module 2: Contamination Threat Management Guide *(December 2003)*
Module 2 presents the overarching framework for management of contamination threats to the drinking water supply. The threat management process involves two parallel and interrelated activities: 1) evaluating the threat, and 2) making decisions regarding appropriate actions to take in response to the threat.

Module 3: Site Characterization and Sampling Guide *(December 2003)*
Module 3 describes the site characterization process in which information is gathered from the site of a suspected contamination incident at a drinking water system. Site characterization activities include the site investigation, field safety screening, rapid field testing of the water, and sample collection.

Module 4: Analytical Guide *(December 2003)*
Module 4 presents an approach to the analysis of samples collected from the site of a suspected contamination incident. The purpose of the Analytical Guide is **not** to provide a detailed protocol. Rather, it describes a framework for developing an approach for the analysis of water samples that may contain an unknown contaminant. The framework is flexible and will allow the approach to be crafted based on the requirements of the specific situation. The framework is also designed to promote the effective and defensible performance of laboratory analysis.

Module 5: Public Health Response Guide *(available March 2004)*
Module 5 deals with the public health response measures that would potentially be used to minimize public exposure to potentially contaminated water. It discusses the important issue of who is responsible for making the decision to initiate public health response actions, and considers the role of the water utility in this decision process. Specifically, it examines the role of the utility during a public health response action, as well as the interaction among the utility, the drinking water primacy agency, the public health community, and other parties with a public health mission.

Module 6: Remediation and Recovery Guide *(available March 2004)*
Module 6 describes the planning and implementation of remediation and recovery activities that would be necessary following a confirmed contamination incident. The remediation process involves a sequence of activities including: system characterization; selection of remedy options; provision of an alternate drinking water supply during remediation activities; and monitoring to demonstrate that the system has been remediated. Module 6 describes the types of organizations that would likely be involved in this stage of a response, and the utility's role during remediation and recovery.

TABLE OF CONTENTS

LIST OF FIGURES

ACRONYMS

AWWARF	American Water Works Association Research Foundation
CDC	Centers for Disease Control and Prevention
ERP	Emergency response plan
ETV	Environmental Technology Verification
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
HazMat	Hazardous materials
ISAC	Information Sharing and Analysis Center
LRN	Laboratory Response Network
PPE	Personal protective equipment
QA	Quality assurance
QC	Quality control
SCADA	Supervisory control and data acquisition
SDWA	Safe Drinking Water Act
TOC	Total organic carbon
URL	Uniform resource locator
US EPA	United States Environmental Protection Agency
UV	Ultraviolet
WCIT	Water contaminant information tool
WUERM	Water utility emergency response manager

GLOSSARY

Definitions in this glossary are specific to the Response Protocol Tool Box but conform to common usage as much as possible.

Agency – a division of government with a specific function, or a non-governmental organization (e.g., private contractor, business, etc.) that offers a particular kind of assistance. In the incident command system, agencies are defined as jurisdictional (having statutory responsibility for incident mitigation) or assisting and/or cooperating (providing resources and/or assistance).

Analytical Approach – a plan describing the specific analyses that are performed on the samples collected in the event of a water contamination threat. The analytical approach is based on the specific information available about a contamination threat.

Analytical Confirmation – the process of determining an analyte in a defensible manner.

Causative Agent – the pathogen, chemical, or other substance that is the cause of disease or death in an individual.

'Confirmed' – in the context of the *threat evaluation* process, a water contamination incident is 'confirmed' if the information collected over the course of the threat evaluation provides definitive evidence that the water has been contaminated.

'Confirmatory' Stage – the third stage of the threat evaluation process from the point at which the threat is deemed 'credible' through the determination that a contamination incident either has or has not occurred.

Consequence – the adverse outcome resulting from a drinking water contamination incident. In the context of the threat management process, the consequence considers both the number of individuals potentially affected as well as the severity of the health effect experienced upon exposure.

Contamination Site – the location where a contaminant is known or suspected to have been introduced into a drinking water system. For example, a distribution system storage tank where a security breach has occurred may be designated as a suspected contamination site. The contamination site will likely be designated as an *investigation site* for the purpose of *site characterization*.

'Credible' – in the context of the *threat evaluation* process, a water contamination threat is characterized as 'credible' if information collected during the threat evaluation process corroborates information from the *threat warning*.

'Credible' Stage – the second stage of the threat management process from the point at which the threat is deemed 'possible' through the determination as to whether or not the threat is 'credible'.

Drinking Water Primacy Agency – the *agency* that has primary enforcement responsibility for national drinking water regulations, namely the Safe Drinking Water Act as amended. Drinking water primacy for a particular state may reside in one of a variety of agencies, such as health departments, environmental quality departments, etc. The drinking water primacy agency is typically the State Health Agency or the State Environmental Agency. The drinking water primacy agency may also play the role of *technical assistance provider* to drinking water utilities.

Emergency Operations Center – a pre-designated facility established by an agency or jurisdiction to coordinate the overall agency or jurisdictional response and support to an emergency.

Emergency Response Plan – a document that describes the actions that a drinking water utility would take in response to various emergencies, disasters, and other unexpected incidents.

Field Safety Screening – screening performed to detect any environmental hazards (i.e., in the air and on surfaces) that might pose a threat to the *site characterization* team. Monitoring for radioactivity as the team approaches the site is an example of field safety screening.

Health Care Provider – any individual or organization involved in the care of patients. Health care providers include physicians and hospitals.

Immediate Operational Response – an action taken in response to a 'possible' contamination threat in an attempt to minimize the potential for exposure to the potentially contaminated water. Immediate operational response actions will generally have a negligible impact on consumers.

Impact – the consequence or effect on drinking water consumers, or the utility itself, resulting from the implementation of response actions. An impact could also be considered as the cost of implementing a response action.

Incident – a confirmed occurrence that requires response actions to prevent or minimize loss of life or damage to property and/or natural resources. A drinking water contamination incident occurs when the presence of a harmful contaminant has been confirmed.

Incident Command System – a standardized on-scene emergency management concept specifically designed to allow its user(s) to adopt an integrated organizational structure appropriate for the complexity and demands of single or multiple incidents, without being hindered by jurisdictional boundaries.

Incident Commander – the individual responsible for the management of all incident operations.

Investigation Site – the location where site characterization activities are performed. If a suspected *contamination site* has been identified, it will likely be designated as a primary investigation site. Additional or secondary investigation sites may also be identified due to the potential spread of a contaminant.

Latency Period – the period of time that elapses between exposure of an individual to a *causative agent* and the appearance of signs or symptoms of disease.

'Possible' – in the context of the *threat evaluation* process, a water contamination threat is characterized as 'possible' if the circumstances of the *threat warning* appear to have provided an opportunity for contamination.

'Possible' Stage – the first stage of the threat management process from the point at which the *threat warning* is received through the determination as to whether or not the threat is 'possible'.

Preponderance of Evidence – an overwhelming and convincing amount of information that is sufficient to conclude that an incident has occurred even though definitive proof may not be available.

Public Health – the health and well being of an entire population or community. Public health does not specifically address the health of individuals.

Quality Assurance – an integrated system of management activities involving planning, implementation, documentation, assessment, reporting, and quality improvement to ensure that a process, item, or service is of the type and quality needed and expected by the client.

Quality Control – the overall system of technical activities that measures the attributes and performance of a process, item, or service against defined standards to verify that they meet the stated requirements established by the client; operational techniques and activities that are used to fulfill requirements for quality.

Rapid Field Testing – analysis of water during *site characterization* using rapid field water testing technology in an attempt to tentatively identify contaminants or unusual water quality.

Response Decisions – part of the threat management process in which decisions are made regarding appropriate response actions that consider: 1) the conclusions of the *threat evaluation*, 2) the consequences of the suspected contamination incident, and 3) the impacts of the response actions on drinking water customers and the utility.

Response Guidelines – a manual designed to be used **during** the response to a water contamination threat. Response Guidelines should be easy to use and contain forms, flow charts, and simple instructions to support staff in the field or decision officials in the *Emergency Operations Center* during management of a crisis.

Security Breach – an unauthorized intrusion into a secured facility that may be discovered through direct observation, an alarm trigger, or signs of intrusion (e.g., cut locks, open doors, cut fences). A security breach is a type of *threat warning*.

Site Characterization – the process of collecting information from an *investigation site* in order to support the evaluation of a drinking water contamination threat. Site characterization

activities include the site investigation, *field safety screening*, *rapid field testing* of the water, and sample collection.

Technical Assistance Provider – any organization or individual that provides assistance to drinking water utilities in meeting their mission to provide an adequate and safe supply of water to their customers. The *drinking water primacy agency* may serve in this capacity.

Threat – an indication that a harmful *incident*, such as contamination of the drinking water supply, may have occurred. The threat may be direct, such as a verbal or written threat, or circumstantial, such as a security breach or unusual water quality.

Threat Evaluation – part of the threat management process in which all available and relevant information about the threat is evaluated to determine if the threat is 'possible' or 'credible', or if a contamination *incident* has been 'confirmed.' This is an iterative process in which the threat evaluation is revised as additional information becomes available. The conclusions from the threat evaluation are considered when making *response decisions*.

Threat Management – the process of evaluating a contamination threat and making decisions about appropriate response actions. The threat management process includes the parallel activities of the *threat evaluation* and making *response decisions*. The threat management process is considered in three stages: 'possible', 'credible', and 'confirmatory.' The severity of the threat and the magnitude of the response decisions escalate as a threat progresses through these stages.

Threat Warning – an unusual occurrence, observation, or discovery that indicates a potential contamination incident and initiates actions to address this concern.

Vulnerability Assessment – a systematic process for evaluating the susceptibility of critical facilities to potential threats and identifying corrective actions that can reduce or mitigate the risk of serious consequences associated with these threats.

Water Contamination Incident – a situation in which a contaminant has been successfully introduced into the system. A water contamination incident may or may not be preceded by a water contamination threat

Water Contamination Threat – a situation in which the introduction of a contaminant into the water system is threatened, claimed, or suggested by evidence. Compare *water contamination threat* with *water contamination incident.* Note that tampering with a water system is a crime under the Safe Drinking Water Act as amended by the Bioterrorism Act.

Water Utility Emergency Response Manager (WUERM) – the individual(s) within the drinking water utility management structure that has the responsibility and authority for managing certain aspects of the utility's response to an emergency (e.g., a contamination threat) particularly during the initial stages of the response. The responsibilities and authority of the WUERM are defined by utility management and will likely vary based on the circumstances of a specific utility.

1 Introduction

The goal of terrorism is to instill fear in the population, not necessarily to cause damage or casualty. This fear can be caused by the mere *threat* of contamination if the threat is not properly managed. For this reason, both threatened and actual contamination *incidents* are a concern faced by the public at large and, in particular, drinking water treatment professionals. Historic evidence suggests that the probability of intentional contamination of the drinking water supply is relatively low; however, experts agree that it is possible to contaminate a portion of a drinking water system, resulting in adverse public health consequences. Furthermore, as discussed in Module 1, the probability of a contamination threat (the mere indication that contamination of the drinking water supply may have occurred) is relatively high. Given that it is possible to contaminate drinking water at levels of public health concern, and the probable occurrence of contamination threats in the water sector, there is a need to evaluate the credibility of any contamination threat and identify appropriate response actions in a very short period of time.

While it is desirable to have complete information prior to making important decisions, the reality is that decisions typically must be made with incomplete information. This will often be the case when responding to contamination threats to drinking water systems since there will not be time to definitively determine whether or not the water has been contaminated with a harmful substance prior to making decisions to protect public health. However, it is also necessary to avoid false alarms that would result in undue panic and stress on the public. Thus a balance must be achieved between actions taken to protect public health and limiting false alarms and overreaction to a perceived threat. FEMA offers an on-line course in decision making and problem solving in emergency situations that may be of interest to the reader (FEMA, 2002)

This module, the "Contamination Threat Management Guide," provides a framework for making decisions based on available, yet incomplete, information in response to a contamination threat. It represents the hub of the "Response Protocol Toolbox," and is supported by the other modules that present procedures for collecting additional information to assist in evaluating the threat or describe various actions that might be taken in response to a contamination threat. Based on this overarching relationship among the modules, the objectives of this module are to:

- Present a framework for evaluating a water contamination threat and making decisions at key decision points in the process.
- Describe the type of information that may be useful for conducting a *threat evaluation*.
- Describe the actions that might be implemented in response to a contamination threat, giving consideration to the potential consequences of an incident and the *impacts* resulting from various response actions.

Based on these objectives, Module 2 is organized into eight sections that deal with the following topics:

Section 1: Introduction: Describes the objectives and overall organization of this module.

Section 2: Overview of the Contamination Threat Management Process: Provides an overview of the process for evaluating a contamination threat and making decisions about appropriate response actions based on the conclusions drawn from the threat evaluation and an analysis of potential consequences.

Section 3: 'Possible' Stage of the Threat Management Process: Describes the general approach for determining whether or not a water contamination threat is '*possible*,' as well as the information sources and response actions that might be considered at this initial stage of the threat evaluation.

Section 4: 'Credible' Stage of the Threat Management Process: Describes the general approach for determining whether or not a water contamination threat is '*credible*,' as well as the information sources and response actions that might be considered at this advanced stage of the threat evaluation.

Section 5: 'Confirmatory' Stage of the Threat Management Process: Describes the general approach for determining whether or not a water contamination incident has been '*confirmed*.' Discusses the information that might be used to confirm an incident as well as the response actions that might be implemented once an incident has been confirmed.

Section 6: Contamination Threat Management Matrices: Presents eight matrices that describe the three stages of a threat evaluation ('*possible*,' '*credible*,' and '*confirmed*') for each type of *threat warning* presented in this module.

Section 7: References and Resources: Lists the references used in the development of this module as well as additional information resources.

Section 8: Appendices: provides a number of forms that support this module and that may be used in the development of a utility's site-specific *Emergency Response Plan* (ERP) or *Response Guidelines* (RGs).

The target audience for this module includes any individuals that might be involved in evaluating the possibility or credibility of a water contamination threat, providing information to support the evaluation, or deciding on appropriate response actions based on the results of the threat evaluation. This will likely include water utility management and staff, *drinking water primacy agency* staff, public health officials, *technical assistance providers*, and law enforcement officers. This module is intended to be a planning tool, and it is recommended that individuals responsible for managing a contamination threat (including an evaluation of the credibility of the threat and response actions to the threat) review this module in its entirety and integrate the concepts presented herein into their own response guidelines.

2 Overview of the Contamination Threat Management Process

This section provides an overview of the entire *threat management* process and serves as a roadmap to the remaining sections of this module. This overview is intended to familiarize the reader with the entire process such that details of the methodology provided in the subsequent sections can be understood in the context of the overall framework. Figure 2-1 is a flow chart depicting the threat management process, which is comprised of two parallel activities: the *threat evaluation* and *response decisions*. While these two activities are interdependent and are performed concurrently during the threat management process, each is presented separately to facilitate the discussion.

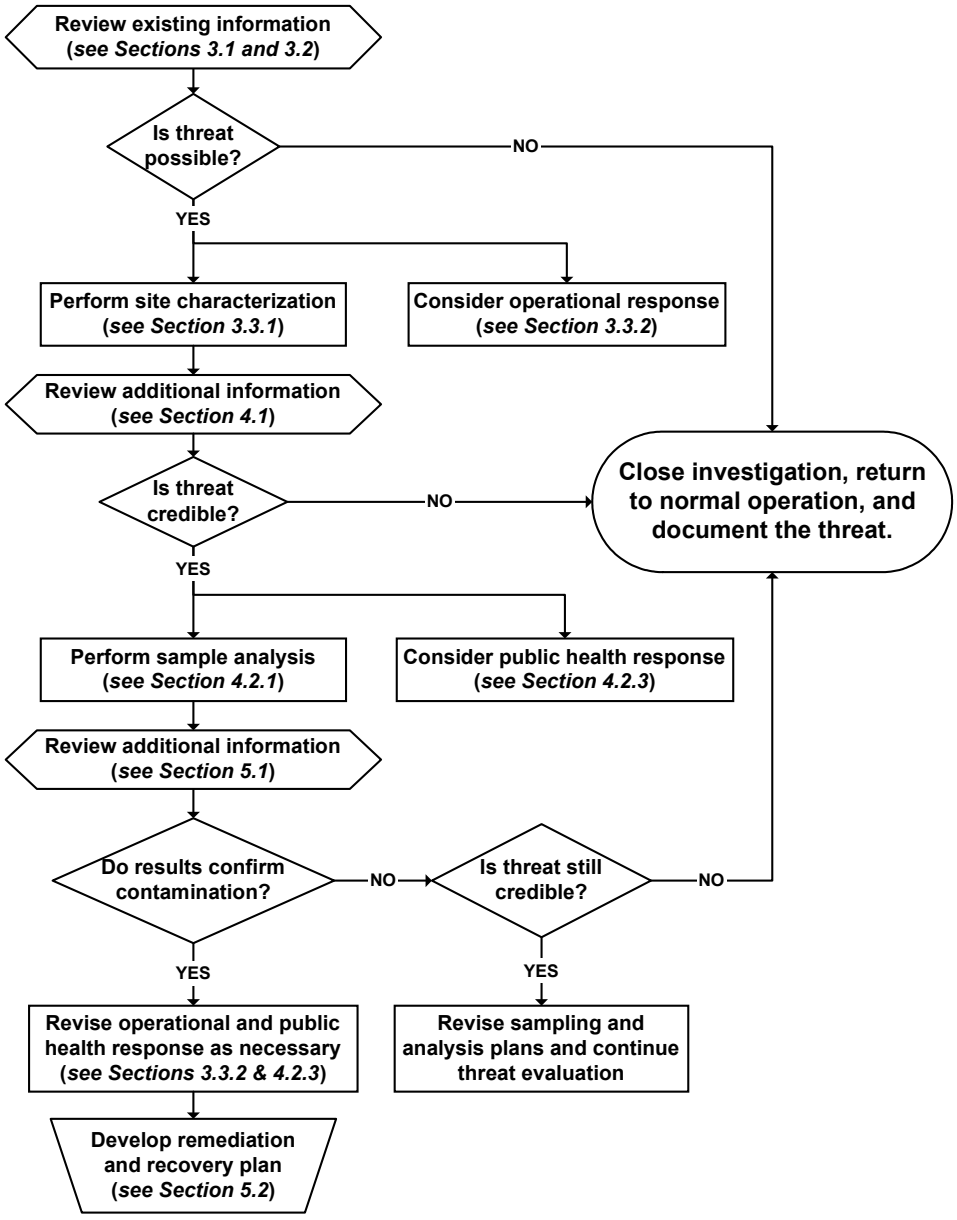


Figure 2-1. Contamination Threat Management Decision Tree

The general decision tree for managing a contamination threat presented in Figure 2-1 is a model that should be applied according to the circumstances of a specific situation. There are numerous discoveries at water facilities that might be interpreted as potential contamination threats, and the decision tree presented in Figure 2-1 is intended to reduce the thousands of potential discoveries to hundreds of possible contamination threats to tens of credible contamination threats. This will in turn allow a utility to respond appropriately to contamination threats that do occur and provide reasonable consideration to the threat without overreacting and triggering harmful false alarms.

2.1 Roles and Responsibilities

Module 1 presented the *Incident Command System* as a model of the organizational structure for managing a contamination threat or incident. Under this structure, the individual with overall responsibility is the *incident commander*. The organization that assumes responsibility for incident command will depend on the nature and severity of the threat or incident. By default, if no other organization with the proper authority assumes responsibility for incident command, it becomes the water utility's responsibility. The *water utility emergency response manager* (WUERM) would assume the role of incident commander in this case.

During the course of managing a contamination threat, the individual designated as incident commander may change as different organizations assume responsibility for managing the situation. For example, during the initial stages of a situation, the WUERM will likely be in the role of incident commander. As more information about the threat becomes available and the situation evolves, different organizations may step in and take command. For example, if terrorist activity is suspected, the FBI will likely assume incident command. On the other hand, if the situation were a potential *public health* crisis (without links to terrorism), the state or local public health agency would likely assume incident command. In cases where another organization has assumed responsibility for incident command, the utility will play a supporting role during the threat management process and maintain responsibility for the system.

The following is a brief discussion of roles and responsibilities during the threat management process. This listing is not intended to be comprehensive for all situations, but to highlight the key players that might be involved in the threat evaluation or in making response decisions.

Drinking Water Utility – The utility will be responsible for incident command, and the WUERM would be designated as the incident commander, unless another organization takes over the situation. As incident commander, the WUERM would be responsible for conducting the threat evaluation and making response decisions. Regardless of the organization responsible for incident command, the utility has an ongoing responsibility as a technical advisor to the incident commander for issues related to the operation of the water system and water quality.

Drinking Water Primacy Agency – This agency may assume responsibility for incident command in cases in which the water utility lacks the resources to manage the threat. The primacy agency may also coordinate some aspects of response and reporting throughout its jurisdiction. Furthermore, the primacy agency may serve as a technical resource to water

utilities and serve as a link to federal resources such as the United State Environmental Protection Agency (U.S. EPA) and the Federal Emergency Management Agency (FEMA).

Public Health Agency (State or Local) – This agency may assume responsibility for incident command in situations in which there is a potential threat to public health. The public health agency will have the lead in coordinating the public health response to a contamination threat or incident, possibly including public notification. They would also have the lead in the public health investigation, including identification of the source of unusual disease or death in the population. The public health agency would also serve as the link to federal resources such as the Centers for Disease Control and Prevention (CDC) and the Laboratory Response Network (LRN). Note: in some states, the state public health agency is also the drinking water primacy agency.

Local Law Enforcement Agency– This agency may assume responsibility for incident command in situations in which criminal activity, excluding federal crimes, is suspected. Law enforcement will have the lead in the criminal investigation and will determine whether or not a crime has been committed. The criminal investigation (i.e., has a crime been committed?) is related to the threat evaluation process, which addresses the more specific question regarding whether or not the water has been contaminated.

Federal Bureau of Investigation (FBI) – This agency ***will*** assume responsibility for incident command when a federal crime, including terrorism, is suspected. Furthermore, FBI will make the determination regarding the credibility of a terrorist threat based on the information available and their experience in criminal investigations. If FBI determines the terrorist threat to be credible, they will assume command of the situation, and the utility will play a technical advisory role.

The roles of federal organizations during the response to an incident are defined in the Federal Response Plan, which is described in Module 1, Appendix 6.2.

2.2 Evaluation of Water Contamination Threats

The process begins with a *threat warning*, which is an unusual event, observation, or discovery that indicates a potential contamination incident and which initiates actions to address this concern. For example, a *security breach* at a distribution system storage tank might be considered a threat warning. A threat warning will typically result in a *threat evaluation*, a process in which all available and relevant information is evaluated to determine the credibility of a contamination threat. The following simple model described the threat evaluation in terms of input, evaluation, and output:

- Input = all available information relevant to the contamination threat.
- Evaluation = systematic evaluation of the **collective** information to determine whether or not the water supply could have been contaminated. It is important to consider all available information as a whole such that any one individual piece of information does not drive the entire decision process.
- Output = conclusions of the threat evaluation (i.e., has something actually happened?).

The threat evaluation is a progressive process that is considered in three stages (or decision points) depicted in Figure 2-1: '*possible*,' '*credible*,' and '*confirmed*.' These stages are briefly described below and discussed more fully in Sections 3, 4, and 5. It is also an iterative process in which the threat evaluation is revised as additional information becomes available. The conclusions from the threat evaluation are considered when making *response decisions*.

The primary focus of the threat evaluation is public health (i.e., has the water been contaminated at levels of public health concern?). However, the threat evaluation should also consider other potential consequences of a contamination incident such as infrastructure damage, adverse impacts on the aesthetic qualities of the drinking water, and reduced consumer confidence.

Management of a contamination threat begins with an evaluation of information about the threat warning. The outcome of this initial evaluation leads to the first decision point in Figure 2-1 – "is the threat possible?" This initial evaluation represents a relatively low threshold that is intended to discriminate between those threats that warrant further investigation and those that can be dismissed as impossible. If the threat is deemed possible, *immediate operational responses* may be implemented to contain the suspect water while the investigation is continued through activities such as site characterization to support the next stage of the threat evaluation. If the threat is not considered 'possible,' the investigation is closed, the threat documented, and the system returned to normal operation.

The results of site characterization and investigation of other sources will yield additional information that will inform the second decision point in Figure 2-1 – "is the threat credible?" This decision represents a higher threshold than that at the *'possible' stage*. In order for a threat to be considered 'credible,' there must be sufficient information and corroborating evidence to indicate that the water may have been compromised. If the threat is determined to be 'credible,' response actions may be necessary to limit the potential for human exposure to the suspect water and law enforcement should be notified due to the potential for criminal activity. The investigation will continue concurrently with these response actions in an effort to confirm the contamination incident. Actions taken to confirm an incident may include the analysis of samples collected during site characterization and/or additional sampling and *rapid field testing*. If the threat is not considered 'credible,' the investigation is closed, the incident documented, and the system returned to normal operation.

The next and final decision point in Figure 2-1 is confirmation of a contamination incident, which will typically be achieved in one of two ways. The preferred approach for confirmation of a contamination incident is through an evaluation of analytical results from samples collected during site characterization. However, this may not always be possible due to the limitations of both sampling and analysis (e.g., sampling may fail to capture an aliquot of the contaminated water). Thus, a contamination incident may also be confirmed through a *preponderance of evidence* indicating that the water has been contaminated. As an example, a contamination incident might be confirmed if there is a security breach with obvious signs of contamination and there are reports of unusual health symptoms in residents near the site of the security breach.

Once a contamination incident is confirmed, it may be necessary to revise protective measures previously implemented in order to ensure that the public will not be exposed to the

contaminated water. Furthermore, it will be necessary to prepare for remediation and recovery activities following confirmation. If the analytical results do not confirm the contamination incident, the credibility of the threat should be reassessed. Upon reassessment, if the threat is **still** deemed credible, it may be necessary to revise the sampling and/or analysis approach since it is possible that the first round of sampling and analysis missed the contaminant. On the other hand, if the threat is no longer considered 'credible' due to negative analytical results and a lack of other evidence, the investigation can be closed, the incident documented, and the system returned to normal operation. However, under such circumstances, it will likely be necessary to collect and analyze a number of samples in the suspect area to provide additional assurance that the water has not been contaminated and is safe to use.

2.3 Consequence Analysis

Effective management of a contamination threat lies in the ability to make appropriate decisions and take appropriate actions in response to the threat. As previously discussed, the credibility of a contamination threat is one consideration in making these response decisions. An equally important consideration is the potential *consequence* to public health. Thus, an analysis of potential consequences associated with a particular contamination threat is a complementary effort to the threat evaluation. Like the threat evaluation, consequence analysis should be viewed as an iterative process since the potential consequences of a particular threat may be better understood as additional information is collected from the ongoing investigation. In conducting a consequence analysis, one should consider the number of individuals potentially affected, the severity of the health effects, and the impact of an interruption in the drinking water supply on consumers.

2.3.1 Number of Individuals Affected

The number of individuals potentially affected by a contamination incident is a function of the spread of the contaminant and the population within the contaminated area. This may be difficult to determine with a great deal of accuracy within the short time period necessary to make response decisions; however, it may be possible to quickly develop a rough estimate using existing information and/or tools. A simple approach is to utilize operational knowledge of the system to approximate the spread of the potentially contaminated water from the point of suspected contaminant introduction. One might also develop a list of typical travel times from key nodes or facilities within the system to large population centers or critical customers.

A more rigorous evaluation approach involves the application of a hydraulic model designed to estimate the spread of a contaminant from a point of introduction through the distribution system. Examples of models that could be applied in this manner include EPA Net, PipelineNet, MWHSoft, Stoner, and Haestad. The capabilities of PipelineNet are described in more detail in Module 5, Appendix 8.7. These models are sophisticated and require a certain level of skill and a significant amount of time to run; thus, it may not be practical to use such models during the early stages of a response to a contamination threat. Furthermore, the successful application of these models depends on knowledge of the location and time of contaminant introduction, information that may not be available in many cases. It may be more useful to run several

scenarios using a hydraulic model as a planning exercise in order to understand how a contaminant might move through a system.

Once the area impacted by the spread of the contaminant has been estimated, the number of individuals potentially affected can be approximated using the population within that area. The population might be estimated from knowledge of the population centers, neighborhoods, and institutions within the bounds of the affected area. Consideration must also be given to the dilution that would occur as a contaminant moves through the system and the relatively small percentage of treated water that is used for consumption. Both of these factors will reduce the number of individuals potentially affected, but not necessarily to levels acceptable to the public.

2.3.2 Health Effects

The severity of the health effects is directly related to the properties and concentration of the contaminant. In cases where the identity of a contaminant is known or assumed, information about its toxicity/infectivity, fate and transport, and resistance to chlorine or chloramines will help in the assessment of potential public health impacts. Health effects might be minor (e.g., minor skin irritation), moderate (e.g., short-term gastrointestinal disease), or severe (e.g., debilitating disease or death). Situations in which there may be sufficient information to make a reasonable assessment of potential health effects include those in which a contaminant is named in a threat, detected through monitoring or analysis, or inferred from clinical data. Information regarding contaminant properties related to public health effects may be obtained from local health authorities, U.S. EPA, and CDC, among others. Unfortunately, in most cases there will not be sufficient information about the suspected contaminant to make an assessment regarding potential health effects. In these instances, it may be appropriate to make the conservative assumption that severe health effects are possible.

2.3.3 Impacts of Response Actions on Consumers

While public health protection is the **primary** objective during management of a contamination threat, it is also important to consider the overall mission of the water utility – to provide a safe supply of drinking water for consumption, sanitation, fire protection, and other consumer needs. Response actions can be taken to minimize possible impacts on public health that could result from an actual contamination incident, but many of these actions will impact the ability of the water system to meet various aspects of its overall mission. For example, if a decision is made to issue a "do not drink" notice, the day-to-day life of citizens will be severely impacted due to the loss of a convenient supply of potable water for consumption and food preparation. Furthermore, if the water is deemed unsafe for fire fighting, an alternate source must be quickly mobilized to maintain fire protection.

2.4 Planning for Response Decisions

Three factors should be considered when planning for decisions regarding actions taken in response to a contamination threat: 1) the credibility of the threat; 2) the potential consequences of the contamination incident; and 3) the impact of the response action on consumers. A "Response Planning Matrix" is a tool that may help decision officials to consider these three

factors when planning for response decisions and might serve as a quick reference guide during an actual crisis. The matrix is a simple tabular summary that lists the three levels of a threat evaluation, the potential consequences of a threat (both the number of people affected and health effects), and potential response actions along with their impacts on consumers. A blank "Response Planning Matrix" is included in Appendix 8.1.

By planning for threats with different levels of credibility and potential consequences, the utility will be better able to make appropriate response decisions quickly. The Response Planning Matrix will also make it clear when response decisions need to be elevated to a higher level within the utility chain of command or coordinated with an external organization, such as the public health agency. Furthermore, an understanding of the potential impacts of various response actions will provide an opportunity to develop strategies for managing and minimizing adverse impacts. For example, the impact associated with issuing a "do not drink" notice might be mitigated through a public awareness program. This outreach approach could educate the public to the possibility of short duration water outages and encourage them to store a supply of emergency drinking water. Such practice is common in areas prone to natural disasters such as earthquakes and hurricanes.

The blank matrix provided in the appendix can be used as an aid during emergency response planning. By working through scenarios with different combinations of credibility, consequences, and impacts, it is possible to gage the relative importance of various factors. For example, it may be determined that the response decisions are influenced more by 'the number of people affected' than the 'health effects.' Since there are a limited number of response actions available to any utility, it is likely that the number of combinations in the matrix will reduce to just a few, and the factors that have the greatest impact on response decisions will become apparent.

Once the planning process is complete, the "Response Planning Matrix" can be completed as necessary to serve as a quick reference guide that could be incorporated in a set of "*Response Guidelines*." The tool may also need to be modified from its current form in Appendix 8.1 to be consistent with a utility's planning process (for example, the "number of people affected" might be changed to "area affected"). During a crisis, such a tool can efficiently guide the WUERM toward appropriate planned response actions under various conditions or scenarios.

3 'Possible' Stage of the Threat Management Process

A water contamination threat is characterized as 'possible' if the circumstances of the threat warning indicate that there was an opportunity for contamination. This is the lowest threshold in the threat evaluation process and is the point at which a decision is made regarding whether or not to proceed with the investigation. If the threat is determined to be impossible, there is no need to continue the threat evaluation or consider any response actions. However, it is likely that many contamination threats will meet this relatively low threshold and thus warrant further investigation.

The target time period for determining whether or not a contamination threat is 'possible' is within **one hour** from the time the threat warning is received by the utility. Given the potentially severe consequences of failing to respond to an actual contamination incident in a timely and appropriate manner, it is important to determine whether or not a threat is 'possible' in this relatively short time frame. The one-hour target, however, should be treated as a flexible goal since the circumstances of a particular threat may dictate a shorter or longer time

As with all stages of the threat management process, the incident commander is responsible for determining whether or not contamination threat is 'possible.' In most cases, this determination will be made by the WUERM, although others may become involved in this initial evaluation as appropriate. For example, if the threat warning is reported by a law enforcement agency, they would likely play a role in determining whether or not a threat is 'possible.' Also, the drinking water primacy agency may wish to be informed about all threat warnings and may participate in this initial stage of the threat evaluation. However, given the short target time frame for this initial evaluation, it is generally recommended that the WUERM have the authority to make this determination and the decision to continue the investigation.

Relevant and timely information is key to determining whether or not a threat is 'possible' in the target time period. In most cases, the information considered at this stage will be derived directly from the threat warning (e.g., type of warning, location, time of discovery, suspected time of incident, and other details). Under some circumstances, additional information beyond the threat warning may be considered. However, there may not be sufficient time to do so in most cases, and the determination regarding whether or not the threat is 'possible' will be based primarily on the details of the threat warning.

3.1 Information from the Threat Warning

A *threat warning* is an unusual event, observation, or discovery that indicates the potential for contamination and initiates actions to address the concern. Threat warnings may come from several sources from both within and outside of the water utilities as shown in Figure 2-2.

Information extracted from details of the threat warning is critical to determining whether or not a contamination threat is possible, and different types of warnings will have different levels of initial credibility. For example, a public health notification of unusual disease or death in the population would have a higher degree of initial credibility than a report of unusual water quality based on general parameters (e.g., pH, chlorine residual, etc.). Some warnings may be judged so

reliable that the threat is deemed 'credible' solely on the basis of information about the threat warning, while others may be almost instantly dismissed as impossible. Each type of threat warning depicted in Figure 2-2 is discussed in greater detail in following subsections, particularly with respect to the initial reliability of the information from such incidents.

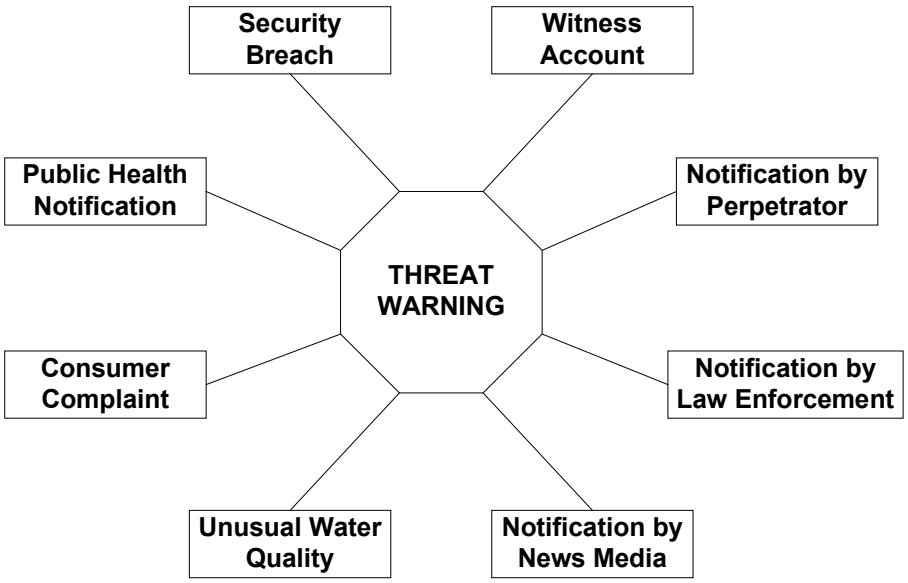


Figure 2-2. Summary of Threat Warnings

Regardless of the nature and source of the threat warning, it is critical that protocols be in place to report the warning to the WUERM as quickly as possible. Utilities and communities should develop communications channels and procedures to ensure that threat warnings can be accurately and quickly reported on 24/7 basis. A "Threat Evaluation Worksheet" is provided in Appendix 8.2 to help organize the information used throughout the threat evaluation, beginning with a summary of information about the threat warning itself.

3.1.1 Security Breach

A security breach is an unauthorized intrusion into a secured facility that may be discovered through direct observation, an alarm trigger, or signs of intrusion (e.g., cut locks, open doors, cut fences). Security breaches are probably the most common threat warnings, but in **most** cases are related to day-to-day operation and maintenance within the water system. Other security breaches may be due to criminal activity such as trespassing, vandalism, and theft rather than attempts to contaminate the water. However, it is prudent to assess any security breach with respect to the possibility of contamination.

When evaluating whether or not a security breach is a possible contamination threat, it is important to consider the circumstances of the incident:

- The mode of discovery of the security breach, e.g., discovery by utility crews, law enforcement, a citizen, security alarm, etc. "Is the source reliable?"

- The time window in which the security breach occurred. "Can a time window be established for the incident based on the times of previous visits to the site and/or the time of discovery?"
- The area in which the security breach occurred. "Is there a history of break-ins, vandalism, or trespassing in this area?"
- Any other information or circumstances about the incident. "Are there signs of theft, vandalism, or mischief?" "Are there indications that multiple individuals were involved?" "Was anything left at the site?"

A "Security Incident Report Form" is included in Appendix 8.3 to assist in documenting the available information about the breach and support the threat evaluation.

If the site of the security breach is equipped with security cameras, the footage should be reviewed as part of the threat evaluation. A video record of the security breach can provide valuable information to help distinguish among normal operational activity, simple trespassing, and 'possible' or 'credible' contamination threats. Furthermore, it can help to establish the actual time of the security breach, which is critical for estimating the area of a distribution system that would be affected if a contaminant were actually introduced (i.e., such information would aid in consequence analysis).

The information about a security breach available at the time of discovery may be sufficient to determine whether or not a threat is 'possible.' However, in most cases additional information will be necessary to determine whether or not the threat is 'credible.' Information collected during *site characterization* activities will be critical to the threat evaluation at this later stage, as discussed in Section 4.1.1.

3.1.2 Witness Account

A threat warning may come from an individual who directly witnesses suspicious activity, such as trespassing, breaking and entering, or some other form of tampering. The witness could be either a utility employee or a bystander. As a result, the witness report may come directly to the utility, or may be directed to a 911 operator or law enforcement agency. If the witness reports the incident to a law enforcement agency, a written or verbal report from the police may provide some insight regarding the possibility of contamination. Furthermore, if the suspect(s) was apprehended, the police report may include additional insight regarding the motives and circumstances of the episode. It is important that the utility establish a relationship with local law enforcement agents, as individuals observing suspicious behavior near drinking water facilities will likely call 911 or law enforcement rather than the water utility.

It is important to collect as much information as possible from the witness to support the initial threat evaluation. A "Witness Account Report Form" is included Appendix 8.4 to help document the witness account. If the witness has not already been interviewed, or if the interview did not cover all aspects of the event that are relevant to the utility's threat evaluation, the WUERM should contact law enforcement and arrange to interview with the witness. In some cases, law enforcement officials may prefer to conduct the interview themselves, but the WUERM may be able to suggest certain questions that are relevant to the threat from the

perspective of the water utility. Information from the witness that would be important to the utility's evaluation includes the number of individuals, their actions at the site, equipment or containers handled by the perpetrators, and anything taken from the site. It is also important to consider the reliability of the source when evaluating information from any witness account,. For example, a threat warning delivered by an individual with a history of filing false reports with police should be considered suspect until corroborated by additional information. On the other hand, direct observation by utility staff would be considered a reliable threat warning.

3.1.3 Direct Notification by Perpetrator

A threat may be made directly to the water utility, either verbally or in writing. Verbal threats made over the phone are historically the most common type of direct threats from perpetrators; however, written threats have also been delivered to utilities. Report forms for both phone and written threats are provided in Appendices 8.5 and 8.6, respectively. A direct notification should be evaluated with respect to both the nature of the threat and specificity of information provided in the threat. In the case of a phone threat, the caller should be questioned about the specifics of the threat: time and location of the incident, name and amount of the contaminant, reason for the attack, the name and location of the caller, etc. The characteristics of the caller should be noted as well (e.g., male/female, accent, tone of voice, background noise, etc.). Given the number of different individuals that might receive a phone threat at a utility, there is a need for training and frequent updates regarding procedures for handling phone threats. In a similar manner, mailroom staff should be provided with training regarding the recognition and handling of suspicious packages and letters. Guidance for dealing with suspicious packages has issued been issued by the US Postal Service (http://www.usps.com/news/2001/press/pr01_1022gsa.htm).

Since tampering with a drinking water system is a crime under the Safe Drinking Water Act, and may involve several other felony acts, any threats received by a utility should be reported to the appropriate authorities, including law enforcement and drinking water primacy agency.

3.1.4 Notification by News Media

A threat to contaminate the water supply might be made through the news media, or the media may discover and report a threat before the utility is alerted. Thus, it is important that utilities establish relationships with the media to emphasize the importance of notifying the utility or the drinking water primacy agency immediately if a threat against the water supply is received. An established contact should be available to receive such calls at any time. If the threat is general (i.e., not targeted at a specific town or city), the utility should evaluate the reported information and may wish to discuss the threat with their primacy agency. The utility may also consider notifying local law enforcement about the general threat.

In the case of a threat against the water supply for a specific city, a conscientious reporter would immediately report the threat to the police, and either the media or the police should immediately contact the water utility. Assuming this level of professionalism in the media, the notification would go directly to the utility or law enforcement. This early notification would provide an opportunity for the utility to work with law enforcement agencies toward assessing the possibility of the threat before any broader notification is made.

Note that a separate report form was not generated for a notification by news media, since this represents a notification pathway rather than a distinct type of threat warning. The "Threat Evaluation Worksheet," and possibly other forms included in the appendices, may be used to document a notification from news media.

3.1.5 Notification by Law Enforcement Agencies

A utility may receive notification about a contamination threat directly from a law enforcement agency. This notification could be a result of suspicious activity reported to the police or a threat to the water supply made through the news media. Other information could also lead law enforcement agents to conclude that there may be a threat to the water supply. In any case, the utility should review the available information with law enforcement to assess whether the threat is possible and decide on appropriate response actions. While law enforcement agents will have the lead in the criminal investigation, the utility has primary responsibility for the safety of the water supply and operation of the water system. Thus, the utility's role will likely be to help law enforcement appreciate the feasibility and public health implications of a particular threat.

Note that a separate report form was not generated for a notification by law enforcement agencies, since this represents a notification pathway rather than a distinct type of threat warning. The "Threat Evaluation Worksheet," and possibly other forms included in the appendices, may be used to document a notification from law enforcement.

3.1.6 Unusual Water Quality

Unusual water quality results may serve as a warning of potential contamination if the data is available in real-time or near real-time. This type of threat warning could come from on-line monitoring, grab sampling, or an early warning system. Appendix 8.7 provides a "Water Quality and Consumer Complaints Report Form," which may be useful when evaluating a threat warning due to unusual water quality.

Unusual water quality data should be evaluated against an established baseline that captures normal variability in the system, both temporally and spatially. Deviations from an established water quality baseline may serve as a threat warning and should be investigated to determine whether or not the results are indicative of potential contamination. In the absence of a baseline, it will be difficult to discriminate between normal variability and legitimate threat warnings – a situation that could lead to unacceptable false alarms. A baseline can be established for any water quality parameter that is routinely monitored, and the following list is intended to be illustrative rather than comprehensive:

- pH of the distributed water is a function of the pH of the finished water at the entry point to the distribution system. In well buffered waters, it will typically remain fairly constant throughout a distribution system in which the water is in equilibrium with the pipe material; however, it may vary if there are corrosion problems.

- Conductivity of the distributed water is a function of the conductivity of the finished water at the entry point to the distribution system. It will typically remain fairly constant throughout a distribution system in which the water is in equilibrium with the pipe material; however, it may vary if there are corrosion problems.

- Chlorine/chloramine residual levels vary as a function of temperature, pH, degree of nitrification, pipe wall demand (i.e., from biofilm or corrosion), and distribution system residence time (i.e., water age). The initial residual is established at the plant and is a function of the disinfectant dose and oxidant demand of the water. Oxidant demand will vary as a function of water quality and typically experiences seasonal fluctuations. The use of disinfectant booster stations in the distribution system must also be considered when evaluating baseline residual data.

- Total organic carbon (TOC) levels in the distributions system will remain relatively constant with respect to the finished water TOC. However, use of strong oxidants, such as ozone, can increase the biodegradable fraction of TOC, potentially resulting in greater variability in TOC levels in the distributions system.

- UV absorbance is typically used as a surrogate for TOC, but is more indicative of the aromatic fraction of TOC. UV absorbance will experience variations similar to TOC and is also impacted by oxidants and disinfectants used in water treatment.

Another factor to consider when establishing a baseline for distribution system water quality is the potential for blending of water quality from different treatment plants. If multiple treatment plants feed the distribution system, the water quality will be a function of the blending ratio of the water from the different plants, in addition to the other factors described above. The task of establishing a baseline for such systems is further complicated by the fact that the blending ratios will vary both spatially and temporally.

Since 9/11, there have been a number of unconventional technologies and parameters suggested as early warning systems that might detect contamination incidents. It is even more important to establish a reliable baseline for an early warning system that relies on such unconventional parameters, since there is not an experience base to support the identification of unusual results without a baseline for comparison. The applicability of on-line monitoring to the detection of intentional contamination incidents is still under study and many questions remain unanswered regarding the applicability of these tools to water security (i.e., general effectiveness, sensor density requirements, false alarm rate, etc.). The topic of on-line monitoring and early warning systems is also discussed in Module 1, Appendix 6.3.

Finally, it is also critical to evaluate a threat warning due to unusual water quality data in light of the performance characteristics of the monitoring and detection equipment. Factors to consider include the rate of false positives, false negatives, known interferences, and instrument reliability. The EPA Environmental Technology Verification (ETV) program has established an on-going program to evaluate the performance of hand held and on-line monitoring and detection technologies. Utilities considering the application of any monitoring technology should evaluate ETV verification reports, if available (www.epa.gov/etv).

3.1.7 Consumer Complaints

An unexplained or unusually high incidence of consumer complaints about the aesthetic qualities of drinking water, or minor health problems resulting from exposure to water (e.g., skin irritation), should be investigated as a potential threat warning. A number of chemicals can impart an odor or taste to water, some may discolor the water, and others might result in minor health problems in exposed individuals. It is also important to realize that a number of chemicals and all pathogens will have no impact on the aesthetic qualities of drinking water; thus, an absence of consumer complaints does not imply that the water is free of contaminants. When evaluating consumer complaints as a potential indicator of contamination, it is important to ask a series of questions:

- Are the complaints significantly different, with respect to number or type, from those associated with typical taste and odor episodes (such as those resulting from lake turnover or algal blooms)?
- What is the specific nature of the compliant? What is the characteristic odor, taste or color? What is the minor health problem experienced by customers?
- Is the reported taste, odor, or color different from those typically reported?
- Is the reported taste, odor, or color characteristic of a particular contaminant?
- Is there an unusual geographic clustering of complaints (e.g., are complaints isolated to a small area of the distribution system)?
- Are the complaints from customers that are not habitual complainers?

The answers to these questions will help to determine whether the complaints are indicative of a possible contamination incident, or typical of normal water quality conditions and routine episodes. Appendix 8.7 provides a "Water Quality and Consumer Complaints Report Form" that may be useful when evaluating a threat warning resulting from unusual consumer complaints.

In order for consumer complaints to be an effective trigger, a utility must have a 24/7 system in place to respond to consumer complaints in a timely fashion. Furthermore, complaint staff should be trained to recognize unusual trends in consumer complaints and have the tools necessary to characterize complaints by type and location. Unusual trends should be reported to the WUERM immediately. A useful resource that describes an approach for investigating consumer complaints as a potential indicator of contamination has been prepared by U.S. Army Center for Health Promotion and Preventative Medicine (2003).

3.1.8 Notification by Public Health Agencies

Notification from a public health agency or *health care providers* (e.g., doctors or hospitals) regarding increased incidence of disease or death is another possible threat warning. This threat warning is obviously contingent on health care professionals associating patterns in exposure and symptoms with potential water supply contamination. A distinction should be made between a notification that comes from public health officials and one that comes directly from health care providers; the former deals with the health of a population, while the latter is concerned with the health of individual patients. Since safe drinking water is a cornerstone of public health, the utility should generally work directly with public health officials rather than individual health care providers. If a threat warning comes in from a health care provider, it should be immediately reported to the local or state public health agency.

A threat triggered by a public health notification is unique in that at least a segment of the population has presumably been exposed to a harmful substance. Given this circumstance, it is likely that public health officials will assume responsibility for incident command and may choose to handle the situation as an epidemiological investigation in an effort to track down the source. During a public health investigation, the utility should work with local or state health officials in a support role.

The role of the drinking water utility will likely be to assist in the evaluation of water as a possible source of the increased disease or death observed in the community. The "Public Health Information Report Form" included in Appendix 8.8 is intended to organize information from public health agencies in a manner to support this evaluation. If the *causative agent* is known (i.e., through clinical data), it may indicate whether or not water is a possible or likely source. For example, if the contaminant is unstable in water, the investigation might focus on other potential sources, such as food.

It is also important to consider the time that would be expected to elapse between exposure and onset of symptoms. If the causative agent is a chemical (including biotoxins and high level radiation), then the time between exposure and onset of symptoms may be on the order of minutes to hours; thus, there is the potential that the contaminant is still present in the water system. On the other hand, the incubation period for most pathogens is on the order of days to weeks, and thus the causative agent may be absent from the system or present only in trace quantities due to water use, dilution, and die-off during the time period between the incident and onset of symptoms. Similarly, the signs of low-level radiation poisoning may not appear immediately following exposure. This time lag will have a significant impact on the response strategy, including both sampling and actions taken to protect public health.

3.2 Additional Information Considered at the 'Possible' Stage

While the threat warning will likely provide the most immediate and relevant information, several other potential resources might be considered at the 'possible' stage. In general, it is assumed that there will only be time to consult resources within the utility at this stage of the threat evaluation given the short time available to determine whether or not the threat is 'possible.' The information resources listed in this section should not be considered comprehensive or mandatory for determining whether or not a threat is 'possible,' since the circumstances of a specific threat are unique and will dictate appropriate information resources. The specific information resources described in this section include:

- Internal utility information from those who know the physical configuration, operation, and typical water quality of the water system.
- Information from the utility's site-specific *vulnerability assessment* that is relevant to the contamination threat.
- Real-time water quality data that might be used as a potential indicator of water contamination, when evaluated in the context of an established baseline.

Even though this information is listed under the 'possible' stage of a threat evaluation, it is important to remember that the analysis of this information will likely continue throughout the

threat evaluation process. Specifically, the same information resources may be used during the 'possible,' 'credible,' and 'confirmed' stages of the threat evaluation, as long as they are relevant. As the investigation continues, additional information will become available and previously collected information may be either confirmed or invalidated. In summary, the threat evaluation process is **continuous** and **iterative** in nature.

3.2.1 Utility Information and Staff Knowledge

Utility staff possess an extensive knowledge about the physical configuration, operation, and water quality of their system. This knowledge should be utilized throughout the entire threat evaluation process, beginning with the assessment of whether or not the threat is 'possible.' Direct experience in dealing with previous security breaches, such as trespassing or vandalism, can provide insight regarding the possibility of contamination during the evaluation of a current threat warning. Knowledge of typical water quality conditions provides a basis for the evaluation of unusual water quality data that might be considered a threat warning. Previous experience with taste and odor episodes may allow staff to recognize unusual patterns in consumer complaints. Furthermore, during advanced stages of an incident, the understanding of distribution system hydraulics by operations staff and engineers will be critical to the rapid assessment of the propagation of a suspected contaminant through a system. In summary, the knowledge and experience of utility staff should be included as a key information resource. Also, the staff can be sensitized to various potential threat warnings so that they can recognize them early and report them to the WUERM in an efficient and timely manner. To facilitate utilization of staff in an emergency, the WUERM should have 24/7 contact information for all critical staff with specialized knowledge of the system.

3.2.2 Vulnerability Assessment

A utility's vulnerability assessment (VA) is another potential source of information to consider during a threat evaluation; however, this will depend on the manner in which the general threat of intentional contamination was addressed during the VA. Information that could be derived from a VA to support the threat evaluation of a specific contamination threat might include:

- Locations potentially considered as high value targets of intentional contamination (e.g., large population centers, government buildings, etc.).
- Locations considered particularly vulnerable to the intentional introduction of contaminants.
- Other site-specific considerations, such as the availability of a particular contaminant in an area.

This information might be of particular value during the evaluation of general contamination threats in which neither a location nor a contaminant is specified or suspected. Ideally, such information would be derived from a VA and summarized as part of utility planning for response to contamination threats (i.e., rather than referring to the complete VA in the midst of a crisis).

3.2.3 Real-time Water Quality Data and Consumer Complaints

Unusual water quality data is a potential threat warning but may also serve as a valuable source of information during the evaluation of a threat triggered by another type of threat warning. For example, a threat warning may result from discovery of a security breach, and real-time (or near real-time) water quality data might be used as an additional source of information during the threat evaluation. Currently, on-line residual disinfectant monitors provide the most likely source of real-time water quality data. However, data from monitoring stations that measure other parameters (i.e., as part of an early warning system) should be evaluated if available. As with water quality data considered as a threat warning, it is important to evaluate water quality data used during a threat evaluation against a baseline and in light of instrument/method performance (see Section 3.1.6 for additional guidance).

Aesthetic characteristics of water are another potential source of information to support a threat evaluation. This information might be most effectively gathered through a review of consumer complaints at the time of the contamination threat. Section 3.1.7 describes the evaluation of information derived from consumer complaints in the context of a threat warning. Appendix 8.7, contains a "Water Quality and Consumer Complaints Report Form" that may be useful during the analysis of such data in support of a threat evaluation.

Given the limited amount of time available to determine whether or not a contamination threat is 'possible,' there may only be time to conduct a cursory analysis of available water quality or consumer complaint data. The analysis of such data should **begin** at the 'possible' stage and continue through the duration of the threat evaluation.

3.3 Response Actions Considered at the 'Possible' Stage

Once a contamination threat has been deemed 'possible,' relatively low level response actions are appropriate. This section describes two response actions that might be considered at this stage: 1) site characterization and 2) immediate operational response. Site characterization is one of the critical activities in the ongoing threat evaluation and is intended to gather critical information to support the 'credible' stage of the threat evaluation. Immediate operational response actions are primarily intended to limit the potential for exposure of the public to the suspect water while site characterization activities are implemented. An example of an operational response action is hydraulic isolation of a tank by pumping water into the tank or valving out a tank. These actions would generally not affect consumers and thus would generally not require public notification.

The decision to implement these response actions must be made very quickly for the actions to have their desired impact. For example, in order for containment to be an effective operational response, it should be implemented as quickly as feasible after a threat is deemed 'possible.' To facilitate this, the WUERM should be empowered to implement such response actions at the possible stage. However, the plans regarding the use of immediate operational response actions should be shared with utility management and all relevant stakeholders (e.g., the drinking water primacy agency).

3.3.1 Site Characterization Activities

Site characterization is defined as the process of collecting information from the site of a suspected drinking water contamination incident. Site characterization activities include the site investigation, *field safety screening*, rapid field testing of the water, and sample collection. The procedures for performing site characterization and sampling are fully described in Module 3, while this section describes the role of site characterization within the overall context of the threat management process. According to Figure 2-1, if initial information from the threat warning indicates that the threat is 'possible,' site characterization activities are performed to gather additional information that will help to establish whether or not the threat is 'credible.' In this respect, site characterization is both a response action (initiated once a threat is deemed 'possible') and an information source (to help determine whether or not the threat is 'credible').

An overview of the site characterization and sampling process is shown in Figure 2-3. The site characterization process is defined in five primary stages:

1. Customizing the Site Characterization Plan to guide the team during site characterization activities.
2. Approaching the Site to perform an initial assessment of site conditions and potential hazards.
3. Characterizing the Site at which point the team performs their detailed site investigation as well as rapid testing of the water.
4. Collecting Samples for possible delivery to a laboratory for analysis.
5. Exiting the Site after completion of all site characterization activities.

The bracketed boxes on the right side of the figure provide additional detail regarding the activities that are implemented during each stage.

The large arrow along the left side of this figure represents the threat evaluation process, and the interconnecting arrows show the interrelationship between the threat evaluation and site characterization processes. Information gathered to support the initial threat evaluation will also support the development of the customized site characterization plan. As site characterization activities progress, information collected from the site will be used to revise and update the threat evaluation. Likewise, the threat evaluation may impact the course of the site characterization activities.

During the development of a site characterization plan, the incident commander (i.e., the WUERM) and other supporting staff should review available information in order to define the *investigation site* and develop an approach for field testing and sampling. A critical consideration during this planning stage is ensuring the safety of the site characterization team. Accordingly, one objective at this point is to conduct a preliminary assessment of potential site hazards. If there are indicators that hazardous contaminants may be involved, then teams trained in hazardous materials safety and handling techniques, such as HazMat teams, should manage and conduct the site characterization. Steps should also be taken to protect the integrity of any potential evidence at the site (e.g, avoid handling or moving potential evidence). Module 3, Appendix 8.1 provides a "Site Characterization Plan Template" that may be useful in developing a customized site characterization plan.

During the approach to the site, the team should look for any evidence of potential contamination and initiate field safety screening. The purpose of field safety screening is to detect any environmental hazards (i.e., in the air and on surfaces) that might pose a threat to the site characterization team. Field safety screening will be conducted based on preliminary information about the threat and potential site hazards. If signs of a hazard are evident during the approach, the team should halt their approach and immediately inform the WUERM regarding their findings. The WUERM may determine that the threat is 'credible' based on this preliminary information, even before site characterization has been completed. Furthermore, if the investigation or field safety screening indicates any acute hazards in the environment, it will be necessary to immediately evacuate the site. In these instances, teams that are properly equipped and trained should deal with the hazard tentatively identified during screening (e.g., HazMat).

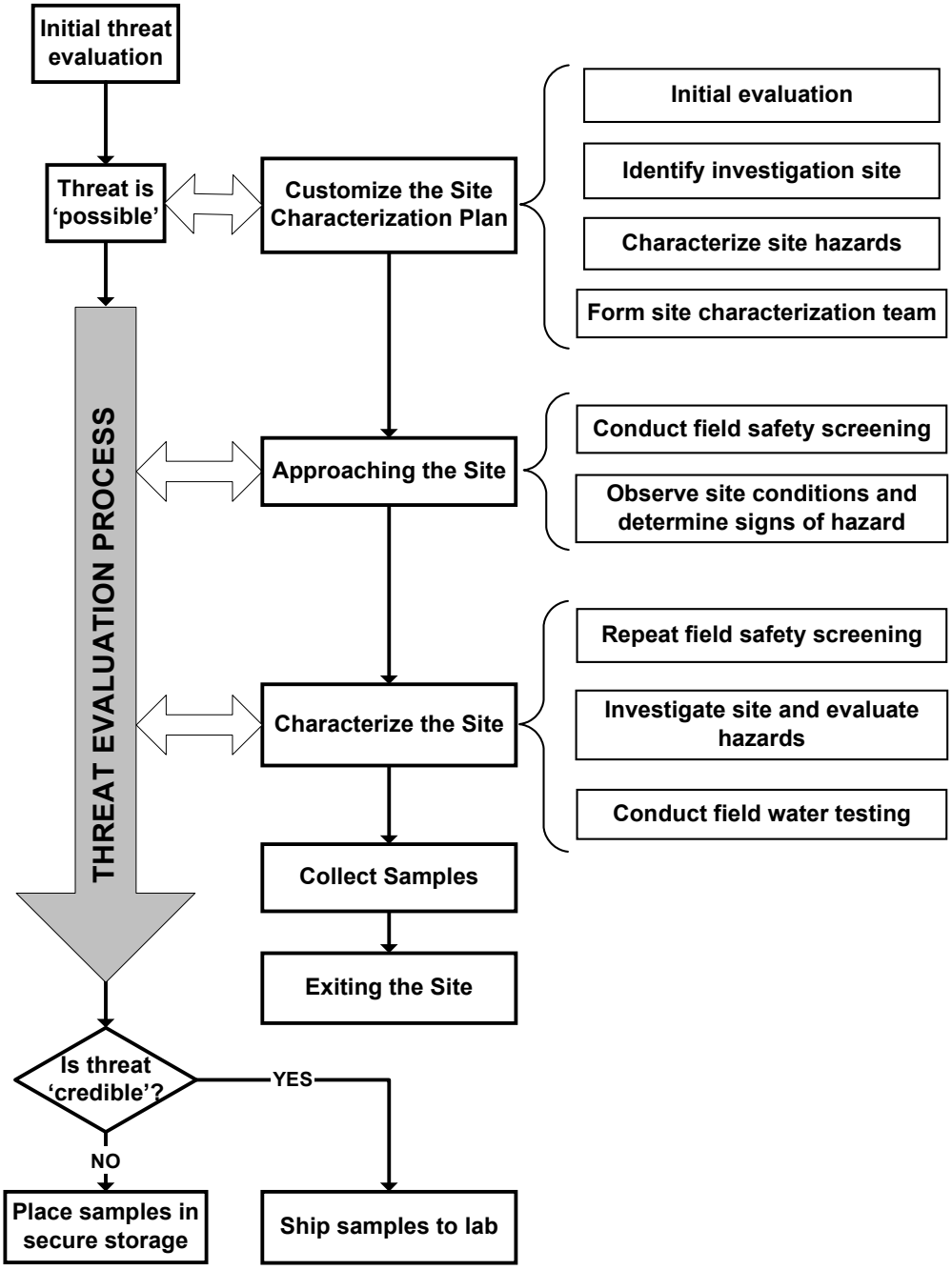


Figure 2-3. Overview of Site Characterization and Sampling Process

In situations where it is deemed necessary to turn over the site to a HazMat team, the WUERM may need to assign a member of the water utility site characterization team to the HazMat team. While it is unlikely that the water utility personnel will be trained in HazMat techniques, they can provide technical advice and guidance to the HazMat responders with respect to water quality, water sampling, and water system components. In some cases the HazMat team may enter the site to perform their hazard assessment and "clear" the site for entry by utility staff.

Once the team has entered the site, they will proceed with the actual site characterization, which includes additional field safety screening, investigation of the site, and rapid field testing of the water. Field safety screening and the site investigation were initiated during the approach and continue when the team enters the site. The primary objectives of rapid field testing of the water include: 1) providing additional information to support the threat evaluation process; 2) providing tentative identification of contaminants that would need to be confirmed in the laboratory; and 3) determining if hazards tentatively identified in the water require special handling precautions.

Following the detailed site characterization, samples should be collected so that they are available for analysis if necessary. Figure 2-3 indicates that the decision to send samples to the laboratory is based on the threat evaluation at the *'credible' stage*. If the threat is deemed 'credible,' the samples should be immediately transported to the laboratory for analysis (see Section 4.2.1 for additional discussion regarding sample analysis). If the threat is not deemed 'credible,' the samples should be stored for a predetermined period of time in case the situation changes and analysis is determined to be necessary.

3.3.2 Immediate Operational Response

The objective of immediate operational response is to minimize the potential for exposure of the public to the suspect water through operational strategies such as containment. These actions are typically suitable for implementation early in the threat management process, assuming that they will have minimal impact on consumers. Furthermore, such response actions may provide the utility with additional time to perform site characterization activities and gather additional information to support the threat evaluation. In general, some form of containment will be the most likely option for an operational response, but other options might be considered as appropriate to a particular situation. Addition guidance on containment can be found in Module 5, Section 4 where containment is considered as a public health response action.

Figure 2-4 provides an overview of the general decision process for implementation of a containment strategy as an operational response to a possible threat. There are three key decision points in the process: 1) Can the area potentially affected by the contaminant be estimated? 2) Is it physically possible to contain the affected area? and 3) Are the impacts of containment on consumers and fire protection minimal? The answers to these questions are influenced by the outcome of the "Consequence Analysis" discussed in Section 2.3.

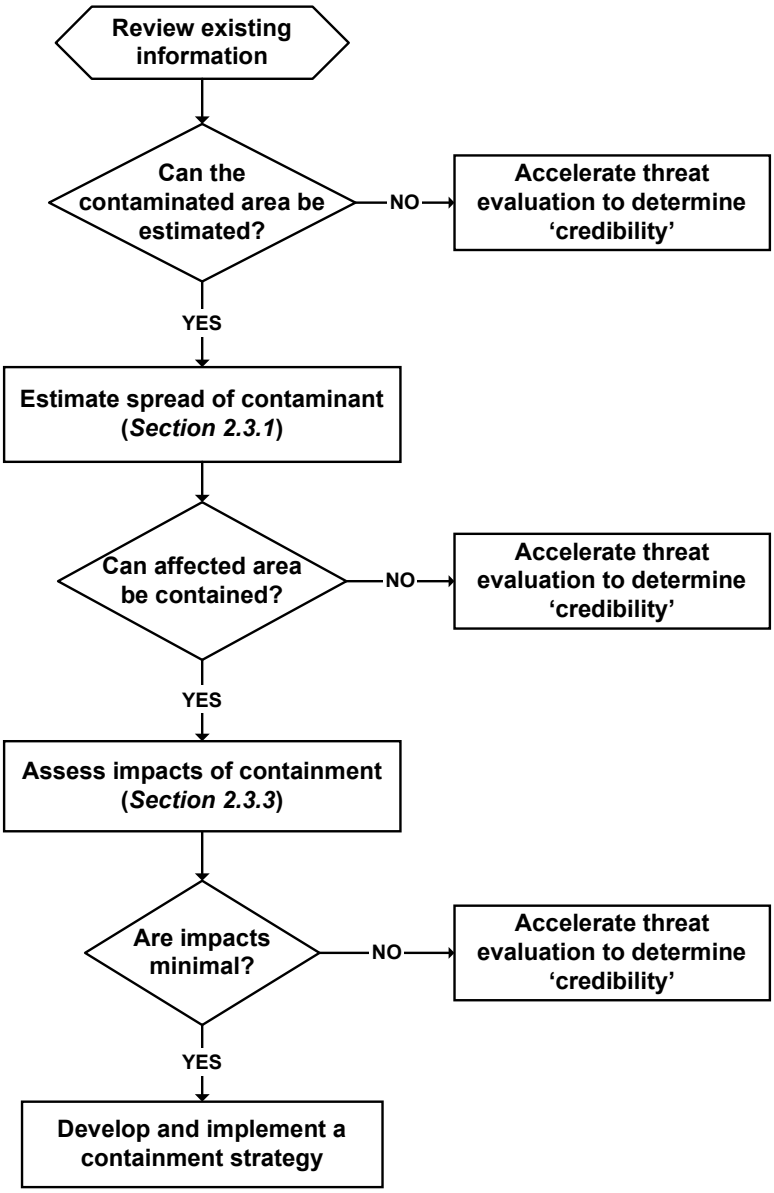


Figure 2-4. Decision Process for Containment as an Operational Response to a 'Possible' Contamination Threat

For containment to be an effective option, the spread of the contaminant must be estimated. This requires knowledge of the suspected location(s) and estimated time(s) of contaminant introduction. These estimates may be derived from the details of the threat warning and other readily available information relevant to the threat. Using the suspected location and time of contaminant introduction as a starting point, the spread of the contaminant through the system can be estimated. Operational information for the system at the suspected location and time may be collected from SCADA, as well as operator knowledge, and will be a valuable resource in estimating the spread of the contaminant. There will generally not be sufficient time to run a hydraulic model for the purpose of estimating the affected area this early in the process. Such

advanced tools may be best used as planning tools where various 'scenarios' can be run to better understand how a contaminant might migrate through a distribution system.

If it is determined that containment is technically feasible and would have minimal impact on the public and on fire protection, then a containment strategy will need to be quickly developed. Utility operations staff will need to engage in both the development and implementation of the containment strategy. Isolation of portions of a system can typically be achieved through hydraulic and/or mechanical means. Hydraulic isolation would typically involve the use of system pumps and pressure zones to contain water within a specific area of the system. Mechanical isolation is achieved through the manipulation of valves, which requires that the valves be accurately mapped and maintained. It is also important to consider how long the isolated area can be kept out of service and plan for alternate routing of water if necessary.

Situations in which containment is likely to be feasible include those in which a specific *contamination site* has been identified and the site can be easily isolated without impacting the normal operation of the system. As an example, some distribution system storage tanks may be isolated using valves without minimal impact on the system pressure. However, there will be many situations in which isolation is not feasible, including situations in which:

- The contamination site is unknown.
- The time of contamination cannot be narrowed down to a reasonable period.
- The extent of the contamination cannot be reasonably estimated.
- The affected area cannot be hydraulically or mechanically isolated.

Furthermore, even if containment is feasible, it may not be practical at the 'possible' stage due to the adverse impacts of isolation on fire protection or sanitation. If containment is determined to be impractical, the threat evaluation should be accelerated to determine whether or not the threat is credible. Once a threat is determined to be credible, expanded response actions might be considered, as discussed in the following section.

4 'Credible' Stage of the Threat Management Process

A water contamination threat is characterized as 'credible' if additional information collected during the investigation corroborates the threat warning, and the collective information indicates that contamination is likely. For example, if the threat warning comes in the form of a security breach and additional signs of contamination are observed during site characterization, the threat would likely be considered 'credible.' While many threat warnings may result in 'possible' contamination threats, only a small percentage of those 'possible' threats are expected to be elevated to 'credible.'

Immediate operational response actions taken once a threat has been deemed 'possible' may decrease the urgency of the situation, but these actions do not constitute resolution of the incident. It is important to move quickly to the next stage of the threat management process to determine whether or not the threat is 'credible' and warrants an elevated response. The target time period for determining whether or not a contamination threat is 'credible' is within **two to eight hours** from the time that the threat is deemed 'possible.' A more precise target time period will depend to some extent on the operational response implemented. If a contaminant strategy was effectively implemented, and there is a degree of confidence that the suspect water did not spread to other parts of the system, there may be more time to make the credibility determination. An example of such a situation is a threat warning resulting from a security breach at a distribution system storage tank that was isolated from the system before the suspect water from the tank had an opportunity to leave the tank and enter the system. On the other hand, if operational response actions cannot be implemented or cannot ensure containment of the suspect water, the threat evaluation process should be accelerated to determine whether or not the threat is 'credible' as quickly as possible.

The decision to elevate a threat from 'possible' to 'credible' is significant since elevated response actions may be necessary to protect public health. These elevated response measures may fall outside of the authority of the WUERM, and the organizations that would be involved in these response decisions would need to be engaged in the threat evaluation process at this stage. This might include water utility management, the drinking water primacy agency, the state/local public health agency, and law enforcement. The person ultimately responsible for determining that a contamination threat is 'credible' is the incident commander, which may not be the WUERM at this stage of the threat management process.

4.1 Information Considered at the 'Credible' Stage

Many of the information resources used to determine that a threat is 'possible' may also prove relevant at the 'credible' stage. Utility information and staff knowledge can aid in the interpretation of new findings from the investigation. Additional water quality data, either real-time or off-line, may be collected and evaluated against baseline data to determine if unusual water quality trends are consistent with the initial data and corroborate the threat. In summary, it is important to view the investigation as a continuum, and the information collected through the 'possible' and 'credible' stages of an investigation should be evaluated in its entirety.

The additional information that might be collected to support the threat evaluation and determine whether or not a threat is 'credible' includes:

- The results of site characterization, including observations from the site investigation as well as results from field safety screening and rapid field testing.
- Summary information derived from an analysis of previous security incidents similar to the current threat warning.
- Information from external sources that is relevant and available in a timely manner.

The following subsections describe each of these information categories in additional detail and discuss how each may be used in support of the threat evaluation process.

4.1.1 Site Characterization Results

In cases in which there is a known or suspected contamination site, site characterization is the focal point of the threat evaluation and potentially provides the most valuable information to support the credibility determination. The findings from site characterization activities should be quickly summarized and provided to the incident commander (which may or may not be the WUERM at this stage) to support the threat evaluation. In Module 3, this summary is referred to as a "Site Characterization Report"; however, it is not intended to be a formal report per se, but may simply be a compilation of the forms completed during site characterization. The information included in the "Site Characterization Report" may include:

- General information about the site.
- Summary of observations from the site investigation including physical evidence (e.g., discarded equipment, containers, etc.) and environmental indicators (e.g., dead animals, dead vegetation, unusual odors, etc.).
- Results from field safety screening and rapid field testing of the water, including any appropriate caveats on the reliability of the results.
- Results of the site hazard assessment.
- Inventory of samples collected and a log of all sampling activities.

The results of field safety screening and rapid field testing of the water warrant special consideration and should be evaluated against baseline data that demonstrates typical variability in the measured parameter. Depending on the parameter monitored, the baseline may vary temporally, spatially, seasonally, or with changing treatment conditions, among other factors. Furthermore, field test results should be evaluated in light of the performance characteristics of the detection equipment such as: the rate of false positive and false negative results; the range in which the instrument or method results are valid; known interferences; and instrument reliability. Deviations from an established baseline that fall within the performance characteristics of the detection equipment may be indicative of contamination. Skill and familiarity with the field testing techniques are required to properly interpret the results. These skills can be reinforced through routine monitoring or exercises with the equipment.

The results of site characterization must be assessed in the context of information previously collected over the course of the threat evaluation. The results of site characterization may corroborate, contradict, or be inconclusive with respect to other information gathered during earlier stages of the incident. **This comprehensive evaluation of information is critical to**

determining whether or not a threat is credible. For example, if the threat warning was a witness account of suspicious activity at a secured location, but no evidence of a security breach was observed during site characterization, the threat would likely be considered 'not credible.' Even though the results of site characterization are critical to the threat evaluation at this stage, it is still important to consider the other available information about the threat, especially if the findings of site characterization are inconclusive.

Another purpose of the site characterization is to conduct a *hazard assessment* of the site, which is an evaluation of the potential presence of immediately dangerous contaminants at the site. Module 3 defines four hazard categories as follows:

- Low hazard – no obvious signs of radiological, chemical, or biological contaminants are present at the site (i.e., in air or on surfaces). Contaminants that may be present in the water are assumed to be dilute and confined to the water.
- Radiological – presence of radiological isotopes or emitters tentatively identified at the site or in the water (i.e., through field safety screening for radioactivity).
- Chemical – presence of highly toxic chemicals (e.g., biotoxins or Schedule 1 chemical weapons) or highly volatile industrial chemicals tentatively identified at the site or in the water that pose a potential risk of exposure through dermal or inhalation routes.
- Biological – presence of pathogens tentatively identified at the site and a potential risk of exposure through dermal or inhalation routes.

The site hazard assessment should incorporate the results of field testing, but not rely exclusively on these results. Observations from the site investigation (e.g., obvious signs of hazards) may be more useful than limited field testing in determining whether or not a site poses an immediate hazard. The findings of the site hazard assessment should be summarized in the 'Site Characterization Report' since they will inform the credibility determination as well as provide direction to subsequent steps of the investigation, such as sample analysis.

4.1.2 Previous Threats and Security Incidents

Information derived from previous threat warnings (i.e., security breaches, phone threats, unusual consumer complaints, etc.) can provide valuable insight regarding the credibility of a current threat. It is equally important to consider those threat warnings that were dismissed as insignificant (e.g., vandalism) as well as those that resulted in an investigation and were deemed 'possible' or 'credible' contamination threats. Such information can be used to corroborate or dismiss a threat; thus it is most appropriate to consider this type of information when evaluating whether or not a threat is 'credible.'

Previous threats and incidents must be documented and catalogued to provide quick access to information that can be used to support a threat evaluation. A comparison between previous incidents and a current threat may indicate whether or not the threat reflects previous patterns and may therefore be deemed 'not credible' (e.g., in the case of repeated vandalism or theft). This documentation could be accomplished through a simple system of filing past reports in an organized and systematic manner. Given the urgency of the threat evaluation process, it is critical that threats be documented and organized when there is time to do so. During emergency

conditions, there will not be time to search through poorly organized or incomplete records in order to further the threat evaluation process.

In addition to a summary of previous threats and security incidents that have occurred at a specific utility, threat information from a regional or national perspective may be of use during a threat evaluation. This information could include results of an analysis of security incidents across the nation, which may be performed by FBI, EPA, AMWA (through ISAC), or AWWA. This type of information might be useful in making general comparisons to the current threat, but will generally not be as relevant as those documented threat warnings that occurred at a specific utility. The types of information that might be available through these and other external sources are discussed in the following section.

4.1.3 Information from External Sources

There are many potential external (i.e., external to the utility) sources of information that may be of value during a threat evaluation. However, as there is insufficient time to identify and pursue new sources during the response to an actual threat, planning is necessary for the effective use of external information sources during a threat evaluation. This planning includes an assessment of the relevance, reliability, and accessibility of each information source prior to the occurrence of a contamination threat. Therefore, it is recommended that a WUERM: 1) identify the information sources that would be used to support a threat evaluation; 2) understand the type of information that the resource might provide; and 3) determine how to access the resource quickly on a 24/7 basis.

The following list provides a summary of external information sources that might be consulted during a threat evaluation. This list is intended to illustrate the value of certain external sources, but is by no means comprehensive. The most relevant information resources will depend on the nature and circumstances of the threat warning, and it is up to the incident commander to apply the information from these various sources in response to a specific threat.

- Drinking Water Primacy Agency: If the Drinking Water Primacy Agency is informed about a contamination threat prior to the credibility determination, they may be of assistance in making this determination. For example, if the primacy agency does track security incidents at water utilities within their jurisdiction, this collective information could be of value when trying to establish the credibility of a threat. Furthermore, the primacy agency may have access to information and expertise for assisting in the threat evaluation process. Also, smaller utilities with limited resources and capability in water security may rely on the primacy agency to perform the threat evaluation.

- EPA: The EPA has a breadth of expertise in drinking water treatment, occurrence and properties of water contaminants, analytical methodology, and remediation of hazardous sites. EPA has also established specific capability in the area of water security in its Water Security Division and National Homeland Security Research Center. Furthermore, EPA's Criminal Investigation Division has experience in the investigation of environmental crimes and links to federal law enforcement agencies. The expertise within EPA can be a valuable resource in responding to a threatened or actual

contamination incident. The best way to access EPA's resources will typically be through the Regional EPA office or the Drinking Water Primacy Agency. Federal expertise, including that from EPA, may also be accessed by calling the National Response Center (NRC) at **1-800-424-8802**. The NRC is the sole point of federal contact for reporting oil and chemical spills and has experts trained to provide assistance in the case of a terrorist threat or incident.

- Law Enforcement Agencies: The expertise of law enforcement agencies (local and State) might be particularly helpful in evaluating the credibility of a contamination threat. They may have knowledge of recent criminal activity in the area that might help establish credibility or support advanced stages of the investigation. It is important to consider that most law enforcement agents have very limited knowledge of drinking water systems, and the WUERM should be available to provide that expertise during the threat evaluation.

- FBI: The FBI may be able to provide support similar to local law enforcement agencies and, in addition, may have access to intelligence information not available to local law enforcement. The focus of the FBI's investigation will be on the criminal or terrorism aspect of the threat, rather than the safety and quality of the water. However, if the FBI determines that the event is credible from a criminal perspective, the threat will likely also be considered credible from a public health perspective.

- Neighboring Utilities: In some cases, neighboring utilities may be a source of information during a threat evaluation. For example, in the case of a threat warning resulting from unusual source water quality, additional insight may be gained by contacting another utility that shares the same source and typically experiences similar water quality. The neighboring utility may be experiencing similar unusual water quality and/or may know the cause.

- Public Health Agencies: Public health agencies may be aware of a significant number of patients showing unusual symptoms or disease through activities such as disease surveillance and reporting. Upon discovering such a trend, the agency may launch an investigation in which they will evaluate how the cases are clustered and search for the cause of the disease. However, in many disease surveillance systems, there is a significant delay between the time that patients begin showing up at hospitals and the time that the public health agency has enough data to observe an unusual trend. Furthermore, there will be a *latency period* between exposure to a contaminant and onset of symptoms, which may range from less than a minute for highly toxic chemicals to over a week for some pathogens.

- 911 Call Centers: 911 call centers may provide consolidated information about unusual signs and symptoms since many members of the public will choose to call 911 for immediate medical assistance. Calls to 911 are even more likely to occur in the case of a chemical poisoning where onset of symptoms is rapid. This information may need to be accessed through law enforcement agencies or an emergency medical service.

- Water ISAC: The Water ISAC is a national resource, available to water-utility subscribers, that serves as a clearinghouse for alerts, warnings, information on drinking water contaminants and other security information released by various agencies. While the information on ISAC may not be immediately relevant to a specific contamination threat at a utility, the collective information on ISAC should create a national picture of the threat level in the water sector and may have information on existing alerts. More detail on the capabilities of the Water ISAC and information regarding how to subscribe can be found at http://www.waterisac.org/.

- Homeland Security Warnings and Alerts: The Department of Homeland Security establishes the national threat level as a general indicator of the potential for terrorist activity and may also issue alerts and warning for specific sectors, such as the water sector. While these warnings and alerts will not be specific to an individual utility, any alerts specific to the water sector or relevant to the circumstances of a particular threat warning may warrant consideration during the threat evaluation.

- Contaminant Information: If a contaminant is named in a threat or tentatively identified during the investigation (i.e., during site characterization), specific information about that contaminant should be consulted to help establish the credibility and potential consequences of the threat. For example, such information can establish whether or not the suspected contaminant is harmful, available, water soluble, stable in water, etc. This information may also support decisions regarding appropriate response actions at the 'credible' stage of the threat management process. A resource for contaminant specific information is the Water Contaminant Information Tool (WCIT). The WCIT is being developed specifically for the water sector and is described in Appendix 8.9. Other sources of contaminant information that might be used in the interim include:
  - http://www.bt.cdc.gov/agent/agentlistchem.asp
  - http://www.cdc.gov/atsdr/index.html
  - http://www.waterisac.org/

4.2 Response Actions Considered at the 'Credible' Stage

The response actions considered at the 'credible' stage may involve more effort and have a greater impact than those considered at the 'possible' stage. This section describes three response actions that might be considered at this stage: 1) sample analysis; 2) continuation of site characterization activities; and 3) public health response. Sample analysis and continuing site characterization are part of the ongoing threat evaluation and are intended to gather information to 'confirm' that a contamination incident did **or** did not occur. Public health response actions are intended to prevent or limit exposure of the public to the suspect water and are more protective and have a greater impact on the public than the operational response actions considered at the 'possible' stage. An example of a public health response action is issuance of a "do not drink" notice.

The incident commander will make decisions regarding actions taken in response to a 'credible' water contamination threat. Due to the elevated level of actions considered in response to a 'credible' threat, responsibility for incident command may be shifted from the WUERM to

another individual or organization at the point when response decisions are made. At this stage, the utility or locality may choose to activate their *Emergency Operations Center* (EOC) to manage the situation, mobilize resources, and institute a more formal incident command structure. Furthermore, the EOC will facilitate a coordinated response among the participating agencies, such as the drinking water primacy agency, state/local public health agency, and local fire and police departments. Activation of the EOC may be full or partial depending on the circumstances.

4.2.1 Sample Analysis

Once a threat has been deemed 'credible,' one of the first steps taken in an effort to confirm a contamination incident is the analysis of samples collected during site characterization. The analytical procedures for confirming the presence of tentatively identified contaminants, or analyzing water samples for unknown contaminants, are presented in Module 4. Given the large number of potential contaminants and the compartmentalized nature of laboratory capability, it will be necessary to make initial decisions regarding the laboratories that will be utilized and the general *analytical approach* that will be used with water samples potentially containing unknown analytes. Note that the presence or suspicion of extremely hazardous substances, as determined through the site characterization, will likely result in other response organizations (e.g., HazMat) becoming involved in the threat management process. These organizations may take responsibility for identifying appropriate laboratories to conduct analyses.

Laboratory selection should be made on the basis of any available information about the threat, the nature of the suspected contaminant, and the hazard assessment performed as part of site characterization. For example, if the site is characterized as a radiological hazard, a radiological laboratory should perform the analytical work. Figure 2-5 shows various categories of laboratories with different analytical capabilities. Laboratories are grouped into two broad categories, chemical and biological laboratories. Chemical labs include general environmental chemistry laboratories, radiological laboratories, and specialty laboratories that may be able to handle exotic contaminants, such as chemical weapons and biotoxins. Biological laboratories include environmental microbiology laboratories and the Laboratory Response Network (LRN) that typically analyze clinical samples for pathogens.

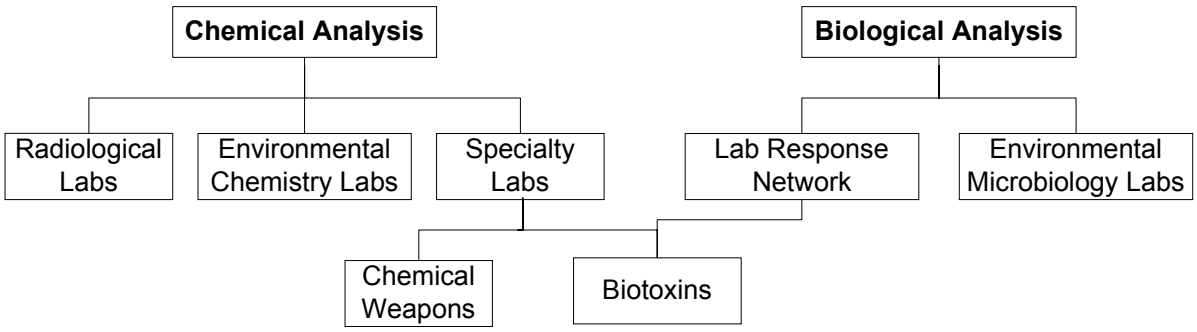


Figure 2-5. Summary of Laboratory Types by Contaminant Class

Once a decision has been made regarding the laboratory(ies) that will be used, the utility and incident commander should work with the laboratory contact(s) to develop an analytical approach for the samples. The approach should be based on all available information about the threat, particularly the results of site characterization. The decision process for developing an analytical approach, which should be planned in advance, is shown in Figure 2-6.

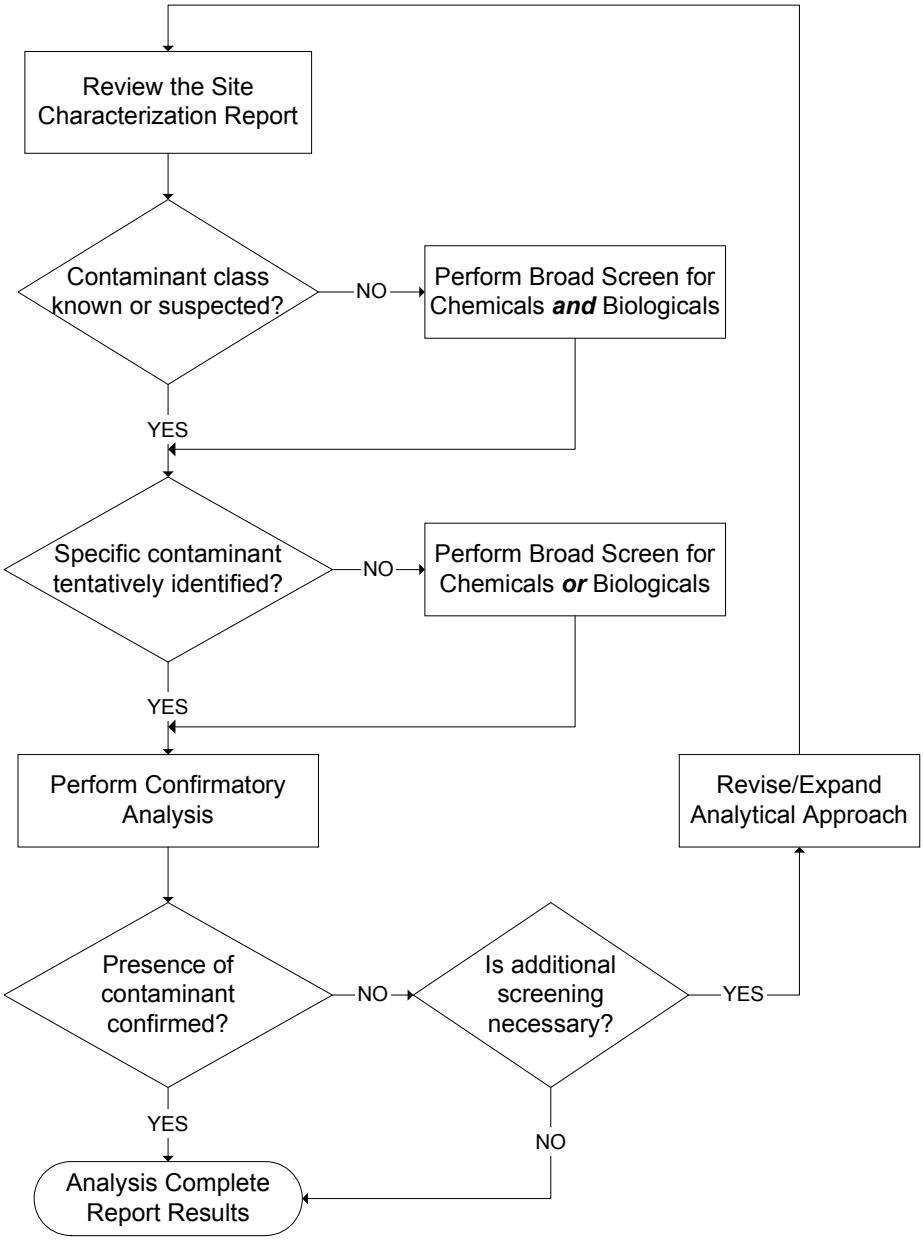


Figure 2-6. Decision Process for the Development of an Analytical Approach for Potentially Contaminated Water Samples

In Figure 2-6, the first decision point in the process is an assessment of whether or not there is sufficient information to make a tentative identification of the contaminant as chemical or pathogen. If this is possible, then an entire class of contaminants is eliminated from consideration, allowing the approach to focus on the tentatively identified contaminant class. If the information is not sufficient to make a determination between chemical and biological contaminants, then the sample may need to be treated as a complete unknown. In this case, it may be necessary to use multiple laboratories (i.e., one lab for chemical analysis and another for pathogen analysis).

The second decision point in Figure 2-6 is based on a tentative identification of the specific contaminant. At this point in the analytical process, the contaminant identity is hypothesized based on available information from the site characterization report or threat warning. Examples of situations in which tentative identification might occur include: a specific contaminant named in a threat; presumptive positive results for a specific contaminant from field screening; physical evidence at the site pointing to a specific contaminant; and clinical evidence of the identity of the causative agent. However, it is important to note that each of these situations has a different level of reliability for the purpose of tentative identification. A tentative identification can be used to focus the analytical approach on confirmation of the specific contaminant or contaminant subclass. For example, tentative identification of a class of pesticides (i.e., organophosphates) may be based on results from a test kit. This information might, in turn, be used to focus the analytical approach on specific pesticides within that class.

The third decision point in Figure 2-6 is based on the results of the analysis used to confirm the presence and concentration of the tentatively identified contaminant. If the presence of the contaminant is analytically confirmed, the contamination incident will also be confirmed. Although not depicted in Figure 2-6, even when the presence of one contaminant has been confirmed, additional analyses may be performed for other contaminants if deemed necessary. The primary purpose of additional laboratory analysis at this point will be further characterization of the contaminated area of the system (see Module 6, Section 4).

If the presence of the tentatively identified contaminant is not verified during confirmatory analysis, the need for additional analytical screening should be considered. Additional screening should be considered since no analytical approach is completely comprehensive. In general, if the threat is still deemed ‘credible’ following negative results from confirmatory analysis, revision to the analytical approach should be considered. Furthermore, it is possible that sampling conducted during site characterization did not capture the contaminated water, and additional sampling may be necessary as discussed in the following section. On the other hand, if the threat is no longer deemed ‘credible’, then additional analysis may be unnecessary.

4.2.2 Continuation of Site Characterization Activities

Site characterization activities initiated in response to a ‘possible’ threat are typically limited to the suspected contamination site with the objective of providing information to support the threat evaluation at the ‘credible’ stage. However, once an incident is deemed ‘credible,’ additional site characterization and sampling activities may be implemented in an attempt to ‘confirm’ a contamination incident. In cases where a ‘credible’ contamination threat is **not** confirmed, the

purpose of additional site characterization and sampling activities will be to verify that the water is safe and support the decision to return to normal operation.

Site characterization activities implemented in response to a 'credible' threat should be planned and coordinated in the same manner as during the 'possible' stage. The scope and extent of site characterization activities at this stage will depend on the available information, and factors to consider include:

- Any information about the identity or nature of the contaminant obtained through laboratory analysis, rapid field testing, or results from the initial site characterization. Such information would help to focus the site characterization activities on the known or suspected contaminant.
- An estimate of the contaminated area through an evaluation of hydraulic information, consumer complaints, water quality data, or other available information. This estimate would help to define the additional locations for site characterization activities.
- Unusual signs or symptoms in the population reported by public health agencies. This information could provide an indication of both the nature and spread of the contaminant. Evaluation of this type of information must consider the latency period between exposure and onset of symptoms.

The available information should help to focus the rapid field testing and sampling activities at this stage. Module 3 contains additional guidance on planning for site characterization activities that is equally applicable to the 'credible' and 'possible' stages of a threat evaluation. In particular, Module 3, Section 3.4 provides some examples that illustrate the transition to follow-on site characterization activities once a threat is deemed 'credible.'

4.2.3 Public Health Response

Like immediate operational response actions, the objective of public health response actions is to minimize the potential for exposure of the public to the suspect water. However, public health response actions are elevated with respect to both the level of protection and the impact on the public. For example, consumers may be instructed to boil water, limit their water uses to activities that do not involve consumption, or not use the water at all. While such measures will provide an increased level of public health protection, they will have a significant impact on consumers. Depending on the duration of these restrictions, it may be necessary to provide an alternate supply of drinking water until the incident is resolved.

Figure 2-7 provides an overview of the general decision process for measures taken to protect public health in response to a 'credible' contamination threat. The first decision point in the process considers containment of the suspect water as a potential public health response action. If containment was implemented at the 'possible' stage as an operational response, the containment strategy should be evaluated to determine if it is adequate to protect public health.

At the 'possible' stage, implementation of containment options was limited by consideration of the impacts of containment on consumers. However, once a threat has been deemed 'credible', expanded containment strategies might also be considered. It may also be appropriate to implement containment strategies and manage the resulting impacts. For example, if there are

consumers within the containment area, it will be necessary to notify them of any restrictions regarding use of their water. In some instances, it may be necessary to provide them with an alternate supply of drinking water.

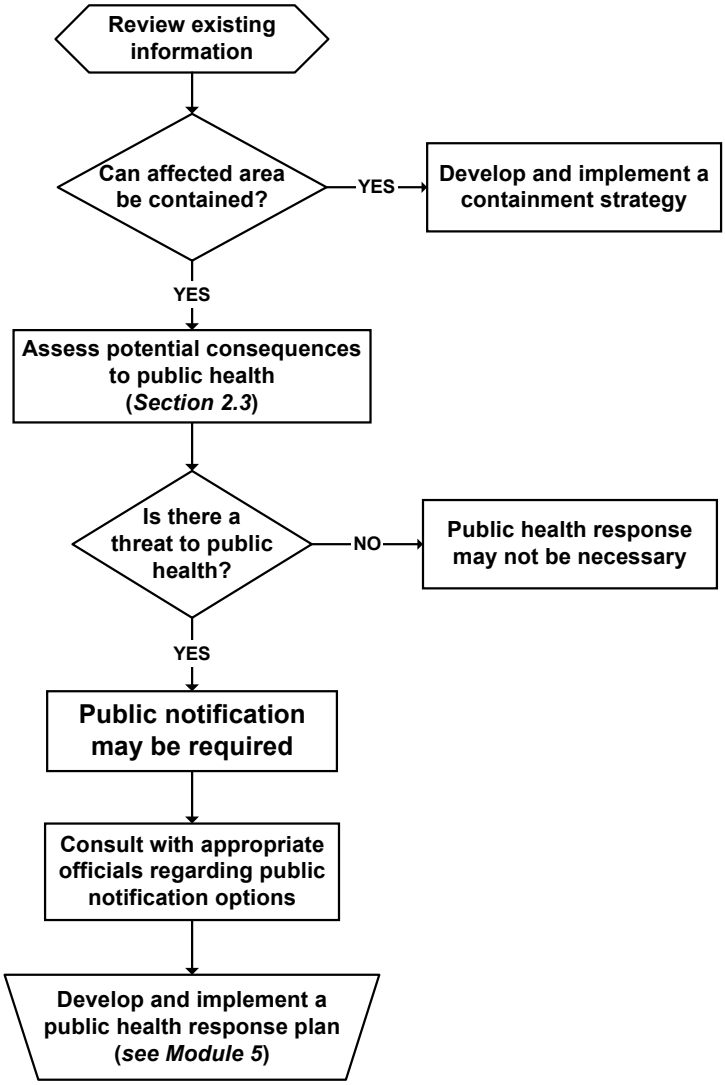


Figure 2-7. Decision Process for Actions taken to Protect Public Health in Response to a 'Credible' Contamination Threat

If containment is deemed inadequate to protect public health, then it is necessary to consider the potential public health consequences of contamination, as discussed in Section 2.3. A "credible threat to public health" results when there is a 'credible' threat **and** the consequences of contamination threaten public health. If it is determined that there is a credible threat to public health, then it may be necessary to notify the public. Furthermore, public notification may be required under the Public Notification Rule (40 CFR Part 141, Subpart Q). Specifically, this rule may require public notification in a "situation with significant potential to have serious adverse

effects on human health as a result of short term exposure" [141.201(b)]. Thus, the utility will need to consult with the drinking water primacy agency, and potentially the public health agency, during the evaluation of public notification requirements and options. Additional guidance regarding public notification and the requirements of this rule can be found in the "Public Notification Handbook" (USEPA, 2002).

Module 5 describes activities related to planning for and implementation of public notifications designed to prevent or limit exposure. Once a decision has been made to notify the public, it is necessary to evaluate the level of notification appropriate for the incident. For example, the level of restrictions on water use that are necessary to protect the public will vary depending on the nature of the contamination. These decisions are influenced by consequence analysis, particularly with regard to the potential health effects of a threat. These potential effects, in turn, are heavily influenced by the identity of the contaminant.

If the contaminant has been tentatively identified at this stage, it may be possible to tailor the public notification to the specific public health risk. For example, if the contaminant only poses a risk through ingestion of contaminated water, a "do not drink" notice may provide a sufficient level of protection. On the other hand, if the identity of the contaminant is unknown, a more restrictive "do not use" notice might be considered. Furthermore, if the public notification places restrictions on the use of the water, it will be necessary to provide a short-term alternate water supply. Of particular concern is the need to maintain fire protection throughout the community. The topics of public notification and alternate drinking water supplies are discussed in detail in Module 5.

5 'Confirmatory' Stage of the Threat Management Process

Confirmation represents the transition from a contamination **threat** to a contamination **incident** and relies on definitive information demonstrating that the water has been contaminated. The most reliable means of confirming a contamination incident is through *analytical confirmation* of the presence of a contaminant. However, under some circumstances, it may be appropriate to confirm a contamination incident in the absence of definitive analytical data. This is particularly true in cases where analytical confirmation may be impractical due to challenges in collecting a representative sample due to uncertainty in the point of contaminant introduction and/or the time that elapsed between the introduction of the contaminant and receipt of the threat warning. In cases where analytical confirmation is deemed impractical, it will be necessary to rely upon the 'preponderance of the evidence' to confirm an incident. A more detailed discussion of this concept is provided below in Section 5.1.

If the threat evaluation yields no conclusive evidence of contamination, then the incident commander may decide that the threat is no longer 'credible.' However, the investigation will have to be sufficiently thorough to demonstrate that the water is safe and the system can be returned to normal operation. Each situation will be unique, and it is up to the judgment and experience of the incident commander and supporting staff to make the determination regarding whether a 'credible' threat is elevated to a 'confirmed' incident or dismissed as 'not credible.'

It may take several days to collect sufficient evidence to confirm a contamination incident, and the required time will depend on the type of information used for confirmation. For example, some microbiological analytical procedures may take several days. The actual amount of time available to confirm the incident will depend on the response actions taken to protect public health once the threat deemed 'credible.'

Due to the magnitude of the effort involved in responding to a confirmed water contamination incident, many organizations will likely be involved in the threat evaluation at this stage. Within the utility, senior managers and the heads of major departments (e.g., operations, water quality, and emergency response) will be involved in this advanced stage of the threat management process. External organizations will likely include the drinking water primacy agency, the state public health agency (if different than the primacy agency), state or local emergency response organizations, and law enforcement agencies. Furthermore, some federal agencies may become involved at this point, and if the governor declares a state of emergency, the Federal Response Plan will become effective and coordinate the federal response (see Module1, Appendix 6.2). While the WUERM will not be responsible for incident command at this stage, it is important for the WUERM to become familiar with the organizations and plans that would be activated in the case of a confirmed contamination incident and to understand the role of the water utility in this situation.

5.1 Information Considered at the 'Confirmatory' Stage

While it is desirable to confirm an incident through laboratory analysis and identification of a particular contaminant, this may not always be feasible. Thus, additional information sources may be considered in an effort to confirm the contamination incident based on a 'preponderance

of evidence.' For example, if there is a security breach with obvious signs of contamination along with unusual water quality and consumer complaints in the vicinity of the security breach, the multiple layers of evidence might be sufficient to confirm a contamination incident. In another situation, additional findings of continued site characterization activities might add to the preponderance of evidence necessary to confirm a contamination incident in the absence of definitive analytical data. The information resources discussed in this section that might support confirmation of a contamination incident include:

- The results from laboratory analysis of samples collected during the initial or continuing site characterization activities.
- The results and observations of continued site characterization activities.
- Information from public health officials, area hospitals, or 911 call centers.
- Information about specific contaminants.
- Targeted information from external sources based on the collective knowledge of the threat.

5.1.1 Analytical Results

Positive identification of a contaminant through sample analysis can confirm a contamination incident and provide the basis for making decisions about public health response actions and remediation activities. Thus, when practical, analytical confirmation should be pursued through a suitable analytical approach as discussed in Module 4. However, all analytical data must be subject to some level of evaluation and interpretation in order to provide meaningful information to support the threat evaluation.

As discussed in Module 4, a report from the laboratory should include the results of all analyses performed, available QA/QC information, and any other information relevant to the interpreting the results. In general, the only analytical results that should be considered at the confirmatory stage of the threat management process are those that have been validated by the laboratory, i.e., the contaminant has been positively identified and/or quantified at the level of concern through the use of accepted analytical methods and QA/QC procedures. If special circumstances warrant consideration of analytical results that have not been validated, it may be necessary to seek laboratory assistance in the interpretation of tentative results. Depending on the analytical methods used, supplementary information provided with non-validated results might include:

- the probability of false negative/false positive results at this stage of analysis;
- method sensitivity, accuracy, and/or precision;
- probability of misidentification;
- quantitative versus qualitative results; and
- the time necessary to confirm the results.

It is important that all of this information be considered when attempting to confirm an incident using data that have not been completely validated.

Furthermore, it is important to consider typical background levels of a particular contaminant during the interpretation of analytical results. However, the availability of background data will likely be limited or nonexistent for many hazardous contaminants. In situations where background data are not available, it may be sufficient to consider occurrence in a more general

sense (i.e., whether the contaminant is known to occur in treated waters). If the general occurrence is unknown, then it may be necessary to evaluate the concentration of the contaminant solely from a public health perspective; specifically, whether or not the contaminant at the levels detected poses any threat to public health.

Interpretation of analytical results for contaminants known to occur in treated drinking water can present unique challenges. For example, chloropicrin and cyanogen chloride are potentially hazardous if present in the water at high concentrations. However, these same compounds are disinfection by-products that result from the reaction of the disinfectant with naturally occurring precursor compounds and thus may occur at very low levels in disinfected drinking water. If low levels of such "normally occurring yet potentially hazardous contaminants" are detected, it must be determined whether these levels represent typical background **or** result from intentional contamination, e.g., the tail of transient contaminant slug or a low-level contamination incident. This uncertainty in the source of the detected contaminant would likely lead to additional sampling and analysis to support the threat evaluation process.

The laboratory should be considered as a potential resource during the interpretation of analytical results. Laboratory staff will have a unique perspective regarding the reliability of the method and interpretation of analytical results as well as substantial experience with the analysis of countless other water samples using the same or similar analytical techniques. Thus, the analyst may have the experience necessary to recognize results that fall within the normal range of occurrence, compared to those more likely to be indicative of an actual contamination incident.

5.1.2 Additional Site Characterization Results

As discussed in Section 4.2.2, site characterization activities may be continued in response to a 'credible' contamination threat to help confirm the incident, or support the decision to return to normal operation if the incident is not confirmed. The focus of continued site characterization would have been influenced by the information already collected through the threat evaluation process; thus, interpretation of the findings may be more straightforward. For example, if unusual water quality results were part of the basis for determining that a threat is 'credible,' additional site characterization activities might be conducted in an effort to confirm the initial findings. Thus, these follow-on site characterization activities will be more focused than the initial site characterization in which there is less information to focus the investigation.

As discussed previously, the results of field safety screening and rapid field testing of the water must be interpreted in the context of background or typical levels, and the reliability of the information must also be considered. Furthermore, the results of additional screening should be compared to the results of the initial screening to determine if they corroborate or contradict the initial results

At the *'confirmatory' stage* of the threat management process, there will likely be results from site characterization activities performed at multiple locations, and these results should be reviewed collectively to explore any potential trends in the data. This may help to build the preponderance of evidence that would be necessary to confirm a contamination incident in the

absence of definitive laboratory analysis. Furthermore, the collective results might provide some indication regarding the spread of the contaminant.

5.1.3 Information from External Sources

Information from external sources can be gathered during the continuing threat evaluation process to support efforts to confirm the incident. At this stage, external resources can be specifically targeted in light of the information already collected to support the threat evaluation. Information from these resources may help to build the preponderance of evidence necessary to confirm an event in the absence of laboratory identification of a contaminant. This information may also support decisions regarding appropriate response actions. The following examples illustrate how external information sources may help to confirm a contamination incident. The other external information sources listed in Section 4.1.3 may also be consulted as appropriate. In any case, it is up to the incident commander and supporting staff to determine how to apply the information from these various sources during the threat evaluation.

- Public Health Sector: In the absence of definitive analytical data to confirm a contamination incident, information from the public health sector may be the next most reliable resource. The occurrence of unusual symptoms in the population or atypical clustering of disease may indicate a potential biological, chemical, or radiological contamination incident. The most immediate source of such information may be through local hospitals and 911 call centers. If there is ample evidence linking these unusual health effects to the drinking water supply, that may be sufficient to confirm the contamination incident. However, water is only one possible source of the contaminant and, in many cases, will not be the primary focus of the public health investigation. The state or local public health agency would typically be the lead agency in the public health investigation and would likely confirm the source of the incident.

- Law Enforcement Agencies: Local and federal law enforcement agencies will probably not be as critical to the 'confirmatory' stage of the investigation as they are at the 'possible' or 'credible' stages. Nonetheless, these agencies will likely still be engaged in the evaluation of a 'credible' threat, particularly as they continue the criminal aspect of the investigation. In particular, they may discover crucial evidence or apprehend a suspect that could help to confirm whether or not the water has been contaminated. Such information would typically not provide definitive analytical confirmation (i.e., it may not reveal the identity of the contaminant); however, it may support confirmation based on a preponderance of evidence. In any case, it is important that the utility remain engaged with law enforcement throughout the investigation.

- Contaminant Information: At the confirmatory stage of the threat management process, information about specific contaminants becomes particularly important. In cases where the contaminant has been identified through laboratory analysis or other definitive means, such information is critical for assessing potential impacts to public health resulting from various routes of exposure to the contaminant. Furthermore, this information will be used to make decisions regarding suitable remediation options. On the other hand, if the contaminant has not been identified, specific information on a number of potential

contaminants might be used in conjunction with other available information in an attempt to narrow down the number of contaminant candidates. For example, if information from site characterization activities indicates that the contaminant impacts water quality in a certain manner (i.e., consumes free chlorine or imparts a certain odor to the water), the contaminant specific information may facilitate tentative identification of a contaminant and inform the analytical approach that would be used in an attempt to positively identify the contaminant. A resource for contaminant specific information is the Water Contaminant Information Tool (WCIT). The WCIT is being developed specifically for the water sector and is described in Appendix 8.9. The WCIT is currently under development, and other sources of contaminant information that might be used in the interim include:

- http://www.bt.cdc.gov/agent/agentlistchem.asp
- http://www.cdc.gov/atsdr/index.html
- http://www.waterisac.org/

5.2 Response Actions Considered at the 'Confirmatory' Stage

Once a contamination incident has been confirmed, it will be necessary to move into full response mode. At this point, the EOC may be fully activated in order to support an effective and coordinated response. Other organizations that may be actively engaged in the response include: the drinking water primacy agency, the public health agency, response agencies, and law enforcement. All of these participating organizations will likely be coordinated under existing incident command structures designed to manage emergencies at the state or local level. One agency will be designated as a lead agency and will be responsible for incident command. If federal agencies are involved in the response, their roles and responsibilities are established by the Federal Response Plan. States and local entities have likely established their own response plans that would be in effect if the incident were managed at that level. In any case, the utility will still have a role in the implementation of full response actions; however, they will generally act in a technical support role.

Figure 2-8 illustrates the actions that might be taken in response to a confirmed contamination incident. The process begins with an evaluation of available information about the incident, which should include identification of the contaminant. Effective implementation of response actions at this stage does depend on positive identification of the contaminant and knowledge of contaminant properties. In particular, the appropriateness of various public health protection strategies and selection of treatment technologies will depend on the nature of the specific contaminant. Due to the potential impact of response actions considered at the 'confirmatory' stage, decision makers may question whether or not the incident has indeed been confirmed if a contaminant cannot be detected in the water. Therefore, it is vital to perform a thorough investigation in order to have confidence in any decisions about response actions. This is especially true if response actions are implemented on the basis of a "preponderance of evidence" rather than analytical confirmation.

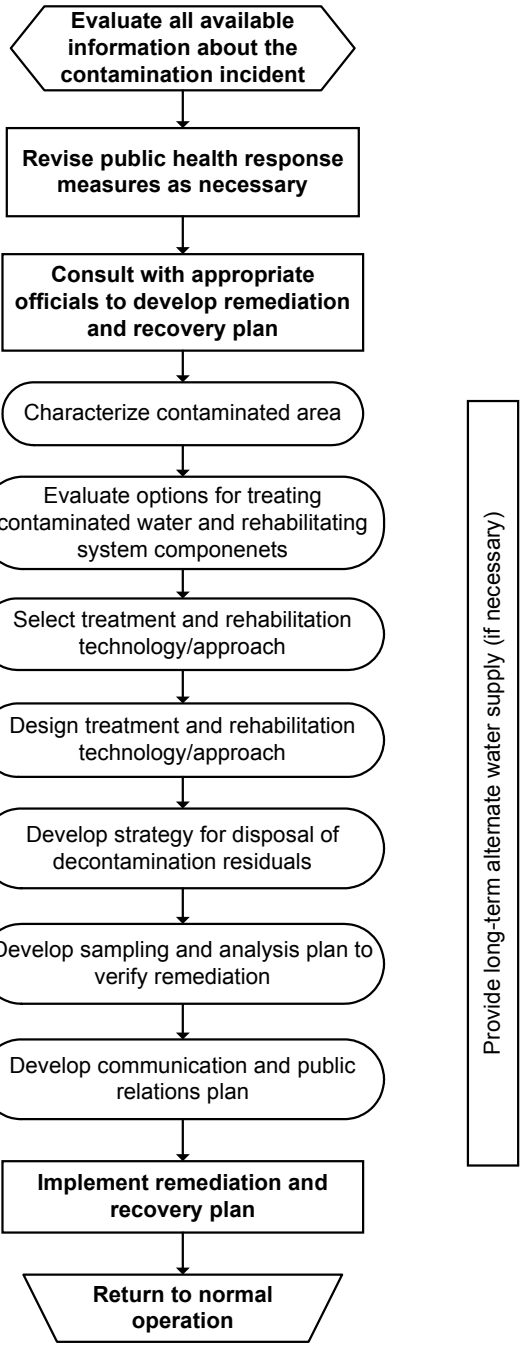


Figure 2-8. Overview of Response to a Confirmed Contamination Incident

Following the initial review of available information about the incident, the public health response measures already implemented should be reassessed and revised if necessary. This process might include revisions to containment strategies or public notifications. This is particularly important if the contaminant has been identified and/or the affected area better characterized following the initial implementation of public health response measures. Once the

immediate public health crisis is under control, efforts will likely focus on remediation and recovery.

Remediation and recovery activities will likely be planned and implemented by a number of agencies, and the first step of the process is to establish the roles and responsibilities of each organization. The elements of the remediation and recovery plan are called out in Figure 2-8 as ovals. Characterization of the contaminated area includes an evaluation of contaminant properties, contaminant concentration profiles, and characteristics of the impacted area. This information is essential to the evaluation of options for treating the contaminated water, remediation of contaminated system components, and disposal of decontamination residuals. The plan should also consider options for supplying alternate drinking water to customers over the duration of the project. Sampling and analysis will be necessary to monitor the progress of treatment and remediation and to ensure that the system is cleaned to acceptable levels by the end of the project. Communications and public relations will be integral to regaining consumer confidence and thus should be considered in the plan as well. Upon successful completion of the remediation effort, the system can begin the process of returning to normal operation. Module 6 describes the remediation and recovery process in detail.

6 Contamination Threat Management Matrices

The previous sections described the three stages of a threat evaluation: 'possible,' 'credible,' and 'confirmatory.' This section compares and contrasts how the information, evaluation, and response options vary as the threat evaluation progresses through the three stages for each of the different types of threat warnings discussed in Section 3.1. For each of these threat warnings, a "contamination threat management matrix" is presented. Each matrix is a tabular summary that lists the following at each stage of the threat evaluation:

- Information considered during the threat evaluation.
- Factors considered during the threat evaluation.
- Potential notifications unique to specific stage of a particular threat warning.
- Potential response actions.

These matrices are necessarily generic and are provided as examples of how the threat management framework described in the previous sections of this module might be applied to specific threat warnings. As part of their planning, users are encouraged to tailor these matrices to their specific circumstances as well as consider threat warnings other than those listed. Furthermore, threat matrices can be developed for more detailed threat scenarios, for example:

- A security breach at a tank that can be isolated from the system.
- A security breach at an uncovered finished water reservoir that cannot be isolated.
- A security breach discovered by an alarm.
- A security breach discovered by utility staff during routine inspection.

Such customized "contamination threat management matrices" could be used as an aid in the development and refinement of ERPs. For example, the completed matrices may indicate the type of response actions that would need to be planned in advance. The customized matrices might also be incorporated into the utility's site-specific "Response Guidelines" and used as a quick reference during the response to a contamination threat.

6.1 Security Breach

	THREAT EVALUATION STAGE		
	Possible	**Credible**	**Confirmatory**
Information	• Location of security breach. • Time of security breach. • Information from alarms. • Observations when security breach was discovered. • Additional details from the threat warning.	• Results of site characterization at location of security breach. • Previous security incidents. • Real time water quality data from the location of security breach. • Input from local law enforcement.	• Results of sample analysis. • Contaminant information. • Results of site characterization at other investigation sites. • Input from primacy agency and public health agency.
Evaluation	• Was there an opportunity for contamination? • Has normal operational activity been ruled out? • Have other "harmless" causes been ruled out?	• Do site characterization results reveal signs of contamination? • Is this security breach similar to previous security incidents? • Does other information (e.g., water quality) corroborate threat? • Does law enforcement consider this a credible threat?	• Were unusual contaminants detected during analysis? Do they pose a risk to the public? • Do site characterization results reveal signs of contamination? • Is contamination indicated by a "preponderance of evidence?"
Notifications	• Notifications within utility. • Local law enforcement agencies.	• Drinking water primacy agency. • State/local public health agency. • FBI.	• Emergency response agencies. • National Response Center. • Other state and federal assistance providers.
Response	• Isolate affected area. • Initiate site characterization. • Estimate spread of suspected contaminant. • Consult external information sources.	• Implement appropriate public health protection measures. • Plan for alternate water supply. • Analyze samples. • Perform site characterization at additional investigation sites.	• Characterize affected area. • Revise public health protection measures as necessary. • Provide alternate water supply. • Plan remediation activities.

Security breaches may be the most common type of threat warning encountered by a utility since they may result from trespassing, vandalism, theft, or failure to re-secure facilities following legitimate activities. The purpose of the threat evaluation under this scenario is to distinguish between these more frequent, yet relatively harmless security breaches, and those few that might be considered 'credible' contamination threats.

At the 'possible' stage of the threat evaluation under this scenario, information about the security breach will be available. Specifically, the location of the security breach will be known, which will likely be established as the initial investigation site. Other information may be available from alarms (including surveillance footage), which may help to establish the time of the security breach. The evaluation at this stage should consider whether or not there was an opportunity for contamination at the site of the security breach. Furthermore, "normal" activity should be considered and investigated at this stage as potential reasons for the security breach (e.g., was a utility crew recently at the site and potentially forgot to re-secure the area?). If the threat of contamination is considered 'possible,' law enforcement agents should be contacted since the security breach may be a result of criminal activity (e.g., criminal trespassing). Potential response actions to a 'possible' threat may include isolating areas of the system that

could be affected, initiating site characterization activities to collect more information in support of the threat evaluation, and initiating the process to estimate the spread of the suspect water through the system.

Information that may be available at the 'credible' stage includes the results of site characterization, an assessment of previous security incidents, real-time water quality data in the area of the security breach, and an assessment of the threat by law enforcement. The evaluation at this stage will consider whether or not signs of contamination were discovered during site characterization, including unusual results from field testing or unusual observations during the site investigation. Consideration should also be given to whether or not the new information available at this stage corroborates the information about the threat. The drinking water primacy agency may be contacted during the 'credible' stage to assist with the threat evaluation and make decisions regarding response actions. (Note: the point at which a primacy agency is notified following discovery of a security breach, or other threat warning, should be consistent with any primacy agency requirements.) The public health agency (if different from the primacy agency) should also be notified if there is a potential threat to public health, particularly since this agency will be able to gather information regarding unusual symptoms in the population and should be involved in any decisions regarding actions taken to protect public health. If the threat is determined to be 'credible,' response actions may include measures to limit or prevent exposure of the public to the suspect water, such as public notification. Actions taken to continue the investigation at this point may include analysis of samples collected from the site, continued site characterization activities, and an analysis to estimate the spread of the contaminant.

The new information available at the confirmatory stage may include the results from laboratory analysis, including QA/QC data to support the interpretation of the results. If a specific contaminant is identified, then additional information about that contaminant can be used to further evaluate the nature of the threat as well as implications to public health. The findings of continued site characterization activities may also help to confirm the incident. The basis for confirming a contamination incident can be analytical results that identify a specific contaminant or other definitive evidence that a contaminant is present in the water. If a contaminant has been identified, consideration should be given to the health effects associated with exposure to that contaminant. It may be necessary to revise the sampling and analysis plans if a contaminant was not positively identified through laboratory analysis but the threat is still deemed 'credible.' Upon confirmation of a contamination incident, a number of agencies that will support the response will need to be notified. Response actions potentially initiated once a contamination incident has been confirmed include characterization of the contaminated area, revision to public health protection measures, provision of alternate water supplies, and planning for remediation and recovery activities.

6.2 Witness Account

	THREAT EVALUATION STAGE		
	Possible	**Credible**	**Confirmatory**
Information	• Location of the suspicious activity. • Witness account of the suspicious activity. • Additional details from the threat warning.	• Additional information from the witness. • Results of site characterization at location of suspicious activity. • Previous security incidents. • Real time water quality data from the location of suspicious activity. • Input from local law enforcement.	• Results of sample analysis. • Contaminant information. • Results of site characterization at other investigation sites. • Input from primacy agency and public health agency.
Evaluation	• Was there an opportunity for contamination? • Is the witness reliable? • Has normal operational activity been ruled out? • Have other "harmless" causes been ruled out?	• Do site characterization results reveal signs of contamination? • Is the suspicious activity similar to previous security incidents? • Does other information (e.g., water quality) corroborate threat? • Does law enforcement consider this a credible threat?	• Were unusual contaminants detected during analysis? Do they pose a risk to the public? • Do site characterization results reveal signs of contamination? • Is contamination indicated by a "preponderance of evidence?"
Notifications	• Notifications within utility. • Local law enforcement.	• Drinking water primacy agency. • State/local public health agency. • FBI.	• Emergency response agencies. • National Response Center. • Other state and federal assistance providers.
Response	• Isolate affected area. • Initiate site characterization. • Estimate spread of suspected contaminant. • Consult external information sources. • Interview witness for additional information.	• Implement appropriate public health protection measures. • Plan for alternate water supply. • Analyze samples. • Perform site characterization at additional investigation sites.	• Characterize affected area. • Revise public health protection measures as necessary. • Provide alternate water supply. • Plan remediation activities.

From the perspective of the threat management process, a threat triggered by a witness account is similar to one triggered by a security breach. One of the few significant differences is the use of information collected directly from the witness throughout the evaluation, particularly during the 'possible' and 'credible' stages of the threat evaluation. As discussed in Section 3.1.2, the reliability of the witness must be considered when making these determinations, and additional evidence collected during the investigation should be evaluated to determine whether or not it corroborates the witness account. In some cases, access to a witness may be restricted by law enforcement agencies, and a direct interview may not be possible. If this is the case, the incident commander should work with law enforcement and make them aware of the type of information that is needed to support the utility's threat evaluation.

6.3 Direct Notification by Perpetrator

	THREAT EVALUATION STAGE		
	Possible	**Credible**	**Confirmatory**
Information	• Transcript of phone (or written) threat. • The who, what, where, when, and why of the threat. • Additional details from the threat warning. • Vulnerability assessment.	• Law enforcement assessment. • Primacy agency assessment. • Previous threats at this utility or other utilities. • Results of site characterization at selected investigation sites. • Real time water quality data. • Reports from ISAC, EPA, etc.	• FBI assessment. • Results of sample analysis. • Contaminant information. • Results of site characterization at other investigation sites. • Input from primacy agency and public health agency.
Evaluation	• Is the threat feasible? • Has the water already been contaminated? • Is the location known or suspected? • Is the identity of the perpetrator known or suspected? • Have there been personnel problems at the utility?	• Do site characterization results reveal signs of contamination? • Does other information (e.g., water quality) corroborate threat? • Does law enforcement consider this a credible threat? • Does the primacy agency consider this a credible threat?	• Were unusual contaminants detected during analysis? Do they pose a risk to the public? • Do site characterization results reveal signs of contamination? • Is contamination indicated by a "preponderance of evidence?"
Notifications	• Notifications within utility. • Local law enforcement. • Drinking water primacy agency.	• FBI. • State/local public health agency. • EPA Criminal Investigation Division.	• Emergency response agencies. • National Response Center. • Other state and federal assistance providers.
Response	• Isolate affected area if identified in the threat. • Identify sites and initiate site characterization. • Consult external information sources. • Gather information from law enforcement assessment.	• Implement appropriate public health protection measures. • Plan for alternate water supply. • Analyze samples. • Perform site characterization at additional investigation sites. • Estimate spread of suspected contaminant.	• Characterize affected area. • Revise public health protection measures as necessary. • Provide alternate water supply. • Plan remediation activities.

Threats to contaminate the water made via direct notification by a perpetrator need to be taken seriously, especially since the mere act of making such a threat is a criminal act. However, the majority of such direct threats are hoaxes that may be intended to cause panic or disruption, gain attention, or meet some personal objective such as revenge. Thus, the focus of the threat evaluation for this type of threat warning is to identify any credible threats amongst the larger number of hoax notifications. In any cases, such threats should generally be reported to law enforcement and the drinking water primacy agency.

A key source of information that may support the threat evaluation under this scenario is provided directly by the perpetrator making the threat, and forms are included in Appendices 8.5 and 8.6 to document phone and written threats, respectively. In the case of a phone threat, it is important to collect information from the caller regarding the threat to support the threat evaluation. Similarly, a written notification should be carefully reviewed for details about the

threat. Additional information collected throughout the investigation should be evaluated against the details of the threat notification. If the additional information collected during the investigation corroborates the details of the threat notification, then the threat is more likely to be considered 'credible.' Furthermore, law enforcement agencies will likely assess the credibility of the threat from a criminal perspective and thus directly support the threat evaluation process. If law enforcement identifies potential suspects, they may take custody of and interview the suspect, and the information gathered during the interview of suspects may be of value during the threat evaluation.

One of the potential challenges in managing a threat triggered by direct notification from a perpetrator is identification of an investigation site that will be the focus of site characterization activities. Unless a location is named in the threat, it will be necessary to use other information, such as that derived from vulnerability assessments or unusual water quality data/consumer complaints, to identify investigation sites. Additional guidance on the selection of investigation sites for site characterization is provided in Module 3.

6.4 Notification by Law Enforcement

	THREAT EVALUATION STAGE		
	Possible	**Credible**	**Confirmatory**
Information	• Law enforcement report. • The who, what, where, when, and why of the threat. • Additional details from the threat warning. • Vulnerability assessment.	• Law enforcement assessment. • Previous security incidents. • Results of site characterization at selected investigation sites. • Real time water quality data. • Reports from ISAC, EPA, etc.	• FBI assessment. • Results of sample analysis. • Contaminant information. • Results of site characterization at other investigation sites. • Input from primacy agency and public health agency.
Evaluation	• How did the threat warning come to law enforcement? • Is the threat feasible? • Has the water already been contaminated? • Is a specific location targeted?	• Do site characterization results reveal signs of contamination? • Does other information (e.g., water quality) corroborate threat? • Does law enforcement consider this a credible threat? • Does the primacy agency consider this a credible threat?	• Were unusual contaminants detected during analysis? Do they pose a risk to the public? • Do site characterization results reveal signs of contamination? • Is contamination indicated by a "preponderance of evidence?"
Notifications	• Notifications within utility. • Drinking water primacy agency.	• FBI • State/local public health agency.	• Emergency response agencies. • National Response Center. • Other state and federal assistance providers.
Response	• Isolate affected area if known. • Identify sites and initiate site characterization. • Work with law enforcement to assess threat credibility. • Consult external information sources.	• Implement appropriate public health protection measures. • Plan for alternate water supply. • Analyze samples. • Perform site characterization at additional investigation sites. • Estimate spread of suspected contaminant.	• Characterize affected area. • Revise public health protection measures as necessary. • Provide alternate water supply. • Plan remediation activities.

Notification of a potential contamination threat by law enforcement may originate from a witness account (reported to a law enforcement agency) or direct notification by the perpetrator, and thus a notification by a law enforcement agency will have some commonalities with these other types of threat warnings. A threat warning coming directly from a law enforcement agent has an initial level of credibility due to the source. However, the specific details should be further evaluated by the WUERM and supporting staff to determine if the threat is indeed possible. Law enforcement agencies will need to rely upon the expertise of drinking water professionals, including those from the utility and primacy agency, to evaluate the threat from the perspective of water quality and public health.

Information used to support the threat evaluation during the 'possible' and 'credible' stages may be derived from the law enforcement agency report and any specific details about the threat that are available. Additional information collected throughout the investigation should be evaluated against the details provided by law enforcement or gained from interviews with witnesses or suspects. Furthermore, any additional information collected should be immediately reported to

law enforcement to aid their ongoing investigation. If the additional information collected during the investigation corroborates the details of the threat warning, then the threat is more likely to be considered 'credible.' The utility will need to work closely with law enforcement agents throughout the threat evaluation in order to determine whether or not the threat is 'credible' and warrants a response.

In some cases, the information about the threat may be sufficient to identify an investigation site. For example, if the notification is a result of a witness account in which suspicious activity was observed at a particular location, it will likely be selected as an investigation site. However, in situations where a site has not been identified, it will be necessary to use other information, such as that derived from vulnerability assessments or unusual water quality data/consumer complaints, to identify investigation sites. Additional guidance on the selection of investigation sites for site characterization is provided in Module 3.

6.5 Notification by News Media

	THREAT EVALUATION STAGE		
	Possible	**Credible**	**Confirmatory**
Information	• Details of media report. • The who, what, where, when, and why of the threat. • Additional details from the threat warning. • Vulnerability assessment.	• Additional details from media. • Law enforcement assessment. • Previous security incidents. • Results of site characterization at selected investigation sites. • Real time water quality data. • Reports from ISAC, EPA, etc.	• FBI assessment. • Results of sample analysis. • Contaminant information. • Results of site characterization at other investigation sites. • Input from primacy agency and public health agency.
Evaluation	• How did the threat warning come to the media? • Is the threat feasible? • Has the water already been contaminated? • Is a specific location targeted?	• Do site characterization results reveal signs of contamination? • Does other information (e.g., water quality) corroborate threat? • Does law enforcement consider this a credible threat? • Does the primacy agency consider this a credible threat?	• Were unusual contaminants detected during analysis? Do they pose a risk to the public? • Do site characterization results reveal signs of contamination? • Is contamination indicated by a "preponderance of evidence?"
Notifications	• Notifications within utility. • Local law enforcement. • Drinking water primacy agency.	• FBI • State/local public health agency.	• Emergency response agencies. • National Response Center. • Other state and federal assistance providers.
Response	• Isolate affected area if known. • Identify sites and initiate site characterization. • Contact news media for additional details. • Consult external information sources.	• Implement appropriate public health protection measures. • Plan for alternate water supply. • Analyze samples. • Perform site characterization at additional investigation sites. • Estimate spread of suspected contaminant.	• Characterize affected area. • Revise public health protection measures as necessary. • Provide alternate water supply. • Plan remediation activities.

In some cases, the news media may be alerted to a threat before the utility. If the threat is generic, the utility may only be able to collect additional information from the media, primacy agency, EPA, ISAC, and other sources to determine if the threat is at all relevant to the specific utility. In the absence of any specifics, the utility may be able to do nothing more than increase vigilance.

If a threat reported by the news media has elements that are specific to a utility, additional information should be collected from the media to help establish whether the threat is 'possible' or 'credible'. Furthermore, the media's information source should be contacted directly if at all possible. It may also be prudent to contact law enforcement agencies early in the process to help determine whether or not the threat is 'possible' or 'credible.' Other than the involvement of the media as an information resource, a threat triggered by notification from news media may be handled in a manner similar to those triggered by other notifications (e.g., directly from the perpetrator or from a law enforcement agency). Additional information collected throughout the investigation should be evaluated against the details of the threat warning. If the additional

information collected during the investigation corroborates the details of the media report, then the threat is more likely to be considered 'credible'.

The media notification may or may not provide information necessary to identify an investigation site. If the media report contains no information about a potential contamination site, it will be necessary to use other information, such as that derived from vulnerability assessments or unusual water quality data/consumer complaints, to identify investigation sites. Additional guidance on the selection of investigation sites for site characterization is provided in Module 3.

6.6 Unusual Water Quality

	THREAT EVALUATION STAGE		
	Possible	**Credible**	**Confirmatory**
Information	• Unusual water quality data. • Baseline water quality data. • Real time water quality data. • Operational information corresponding to the time of the unusual water quality.	• Results of site characterization at selected investigation sites. • Previous threat warnings triggered by water quality. • Contaminant information. • Reports of consumer complaints.	• Results of sample analysis. • Contaminant information. • Results of site characterization at other investigation sites. • Input from primacy agency and public health agency.
Evaluation	• Is the unusual water quality significantly different from an established baseline? • Could operational changes be the cause? • Could changes in source water quality be the cause? • Are there similar results at other monitoring locations?	• Do site characterization results reveal signs of contamination? • Is this unusual data substantial different from other water quality episodes? • Is the unusual data indicative of a specific contaminant? • Are the unusual water quality clustered in a specific area? • Are there any unusual consumer complaints in the area?	• Were unusual contaminants detected during analysis? Do they pose a risk to the public? • Do site characterization results reveal signs of contamination? • Is contamination indicated by a "preponderance of evidence?"
Notifications	• Notifications within utility.	• Drinking water primacy agency. • State/local public health agency. • Local law enforcement. • FBI.	• Emergency response agencies. • National Response Center. • Other state and federal assistance providers.
Response	• Identify sites and initiate site characterization. • Begin analysis of available water quality data. • Investigate unusual consumer complaints. • Consult external information sources.	• Estimate affected area and isolate if possible. • Implement appropriate public health protection measures. • Plan for alternate water supply. • Analyze samples. • Perform site characterization at additional investigation sites.	• Characterize affected area. • Revise public health protection measures as necessary. • Provide alternate water supply. • Plan remediation activities.

A threat warning arising from unusual water quality data is **significantly different** from the other threat warnings previously discussed and thus should be handled differently during the threat evaluation. In determining whether or not the threat is possible, it is necessary to evaluate the anomalous data relative to an established baseline. Furthermore, it is important to consider operational conditions, or potential impacts from changing source water quality or distribution system blending as possible explanations for the unusual water quality. If the unusual water quality data is determined to be significantly different from the baseline, and cannot be explained by other factors, then the threat of contamination should be considered a possibility. In order to proceed with the threat evaluation in a timely manner, the supporting information, such as baseline water quality data, must be summarized in a useful, predetermined format that facilitates a rapid assessment of the suspect water quality data.

Presumably, the unusual water quality data will be associated with a particular location in the system, which will help in the identification of investigation sites that will be the focus of site characterization activities. At this stage of the incident, it is important to verify the anomalous water quality data through additional testing using independent equipment. For example, if an incident was triggered by a rapid decrease in the free chlorine residual, as detected by online electrochemical monitors, additional testing could be performed with colormetric field kits to confirm the results. Additional rapid field testing might also help to determine the bounds of the affected area. Furthermore, additional data collected during the investigation should be evaluated to determine whether or not it corroborates the unusual water quality data. Specific information about particular contaminants should be considered at the 'credible' stage as it might be used to identify potential contaminants that would impact the water quality parameter with anomalous readings. For example, contaminants with acidic functional groups might result in reduced pH.

The investigation of unusual water quality will likely remain within the utility until sufficient information has been gathered to indicate that there is a credible contamination threat. Water quality changes constantly due to a number of complex and interrelated factors, and it is appropriate that most of these water quality episodes be investigated within the utility. However, it is equally important to recognize a significant, unusual, and unexplained change in water quality and investigate the cause. If over the course of the investigation, corroborating evidence is found to indicate a 'credible' contamination threat, then additional notification outside of the utility may be appropriate.

6.7 Consumer Complaint

	THREAT EVALUATION STAGE		
	Possible	**Credible**	**Confirmatory**
Information	• Compilation of consumer complaints, including geographic distribution. • Recent water quality data that may be associated with complaints. • Operational information corresponding to the time of the unusual complaints.	• Results of site characterization at selected investigation sites. • Summary of historic consumer complaints. • Results of consumer interviews. • Contaminant information.	• Results of sample analysis. • Contaminant information. • Results of site characterization at other investigation sites. • Input from primacy agency and public health agency.
Evaluation	• Are the complaints unusual? • Could operational changes be the cause? • Could changes in source water quality be the cause? • Are the complaints clustered in a specific area? • Are complaints from habitual complainers?	• Do site characterization results reveal signs of contamination? • Are other consumers in the area experiencing similar water quality? • Are the unusual complaints significantly different from typical complaints? • Are the complaints indicative of a specific contaminant? • Is there anything unusual about the water quality in the area?	• Were unusual contaminants detected during analysis? Do they pose a risk to the public? • Do site characterization results reveal signs of contamination? • Is contamination indicated by a "preponderance of evidence?"
Notifications	• Notifications within utility.	• Drinking water primacy agency. • State/local public health agency. • Local law enforcement agency. • FBI.	• Emergency response agencies. • National Response Center. • Other state and federal assistance providers.
Response	• Identify sites and initiate site characterization. • Begin analysis of available water quality data. • Interview consumers in area with high numbers of complaints. • Consult external information sources.	• Estimate affected area and isolate if possible. • Implement appropriate public health protection measures. • Plan for alternate water supply. • Analyze samples. • Perform site characterization at additional investigation sites.	• Characterize affected area. • Revise public health protection measures as necessary. • Provide alternate water supply. • Plan remediation activities.

If a utility has a system for tracking consumer complaints, then there is the potential that a high or unusual incidence of consumer complaints could serve as a warning of a possible contamination incident. This is especially true for chemical contaminants, which, depending upon the concentration, may impart a strong odor/taste or discolor the water. In many respects, a threat warning resulting from consumer complaints is similar to one resulting from unusual water quality, particularly when one considers that consumer complaints are simply a surrogate indicator for the aesthetic qualities of drinking water. Furthermore, consumer complaints must be evaluated against baseline information about complaints in order to determine if they are indicative of a 'possible' contamination threat. Other factors that might impact aesthetic water quality, or consumer complaints, should also be considered when determining whether or not the

threat is 'possible.' For example, operational changes or normal source water events, such as algal blooms, could be the cause of the complaints.

In order for consumer complaints to be an effective trigger, a utility must have a system in place that responds to consumer complaints in a timely fashion and have an established communication link to the WUERM. Furthermore, an effective system would be operational 24/7 with staff trained in recognizing contaminant characteristics such as unusual odors and able to characterize complaints by type and location.

If there is a geographic clustering of complaints, this will assist in the identification of investigation sites that will be the focus of site characterization activities. Available online water quality data and rapid field testing results should be evaluated to determine whether or not the information corroborates or explains the aesthetic changes in the water. Furthermore, other customers in the same area might be questioned regarding the aesthetic qualities of their drinking water. If the additional information collected during the evaluation indicates that contamination is likely, then the threat will likely be deemed 'credible.'

6.8 Public Health Notification

	THREAT EVALUATION STAGE		
	Possible	**Credible**	**Confirmatory**
Information	• Details of notification from public health sector. • Symptoms of disease and causative agent, if known. • Contaminant information.	• Geographic distribution of disease or death. • Recent water quality and operational data. • Reports of consumer complaints. • Contaminant information.	• Results of site characterization at selected investigation sites. • Results of sample analysis. • Contaminant information. • FBI assessment.
Evaluation	• Why is water under investigation as a possible source? • Are the reported symptoms consistent with exposure to the contaminant via water? • If causative agent is known, is it stable in water?	• Is the geographic pattern of exposure consistent with exposure to contaminated water? • Is there a recent occurrence of unusual water quality data or consumer complaints? • Does additional information about the potential contaminant indicate water as a potential source?	• Has the public health agency concluded that water is the cause of the disease or deaths? • Did sample analysis detect the causative agent? • Was another contaminant detected during sample analysis that could be the cause of the disease or deaths?
Notifications	• Notifications within utility. • State/local public health agency. • Drinking water primacy agency.	• FBI. • Local and State law enforcement agencies.	• Emergency response agencies. • National Response Center. • Other state and federal assistance providers.
Response	• Consult with public health agency and primacy agency. • Consult external information sources.	• Estimate affected area and isolate if possible. • Implement appropriate public health protection measures. • Plan for alternate water supply. • Identify sites and initiate site characterization. • Analyze samples.	• Characterize affected area. • Revise public health protection measures as necessary. • Provide alternate water supply. • Plan remediation activities.

Notification from public health regarding a potential water contamination incident is unique in that individuals have been exposed to a harmful substance resulting in illness, disease or death in the population. The threat evaluation in this case may be part of a larger epidemiological investigation to determine the cause of disease. From a utility perspective, the first step will be to evaluate whether or not the drinking water is a possible source of the harmful contaminant. It is critical that the utility work with the appropriate public health officials from the outset, since these officials will likely have information critical for the evaluation. For example, they may know or suspect the causative agent based on clinical information. This knowledge, in conjunction with information about the properties of the contaminant, may indicate whether or not contaminated water is even a possibility. For example, if the causative agent is known to immediately decompose upon exposure to water, then the possibility of contaminated water might be dismissed.

If water is considered a possible carrier for the contaminant, then further investigation should be conducted to determine if water is the most likely carrier of the contaminant (i.e., analogous to

the 'credible' stage of the threat evaluation). Information that may help to make this determination will include additional findings from the larger epidemiological investigation, geographic distribution of exposure, recent water quality and operational data, and reports of consumer complaints. If this additional information indicates that water contamination is likely, response actions would likely include public notification to limit further exposure as well as sampling for the suspected contaminant.

The sampling plan developed at this point may start with information about the geographic distribution of exposure; however, consideration must be given to the latency period of the disease, which could be from minutes to weeks, as well as the travel time within the system. The objectives of sampling and analysis at this point would include: 1) confirming the presence of the contaminant in the water; 2) determining if the contaminant is still present; and 3) determining the area affected. If water contamination is confirmed, and the contaminant is still present in the system, it will be necessary to begin planning for remediation and recovery efforts. If the contaminant is not found, extensive sampling would likely be necessary to demonstrate that the contaminant is indeed absent from the system.

7 References and Resources

References and information cited or used to develop this module are listed below. The URLs of several sources are cited throughout the text. These URLs were correct at the time of the preparation of this document. If the document is no longer available at the URL provided, please search the sponsoring organization's Web site or the World Wide Web for alternate sources. A copy of referenced documents may also be provided on the CD version of this module, although readers should consult the referenced URL for the latest version.

AWWARF, 2002. Online monitoring for drinking water utilities. Editor, Erika Hargesheimer, AWWA Research Foundation and CRS PROAQUA, American Water Works Association, Denver, CO; ISBN 1-58321-183-7.

FEMA Emergency Management Institute. http://training.fema.gov/EMIWeb/IS/crslist.asp.

U.S. Army Center for Health Promotion and Preventative Medicine, 2003. "Drinking Water Consumer Complaints: Indicators from Distribution System Sentinels, TG 284. http://chppm-www.apgea.army.mil/documents/TG/TECHGUID/TG284.pdf.

U.S. EPA. 2000. 40 CFR Part 141, Subpart Q. National Primary Drinking Water Regulations: Public Notification Rule; Final Rule. *Federal Register* (Part II). 65(87): 25982-26049. http://www.epa.gov/safewater/pws/pn/pnrule.pdf.

U.S. EPA. June 2000. Public Notification Handbook. EPA/816/R-00/010. Office of Water. Washington DC. http://www.epa.gov/safewater/pws/pn/handbook.pdf.

8 Appendices

8.1 Response Planning Matrix

Incident				**Response**	
Credibility	*Consequences*		*Other Considerations*	*Possible Actions*	*Anticipated Impacts on the public*
	# people affected	*Health Impact*			
Possible	10's	Minor			
		Moderate			
		Severe			
	100's	Minor			
		Moderate			
		Severe			
	1,000's	Minor			
		Moderate			
		Severe			
Credible	10's	Minor			
		Moderate			
		Severe			
	100's	Minor			
		Moderate			
		Severe			
	1,000's	Minor			
		Moderate			
		Severe			
Confirmed	10's	Minor			
		Moderate			
		Severe			
	100's	Minor			
		Moderate			
		Severe			
	1,000's	Minor			
		Moderate			
		Severe			

8.2 Threat Evaluation Worksheet

INSTRUCTIONS

The purpose of this worksheet is to help organize information about a contamination threat warning that would be used during the Threat Evaluation Process. The individual responsible for conducting the Threat Evaluation (e.g., the WUERM) should complete this worksheet. The worksheet is generic to accommodate information from different types of threat warnings; thus, there will likely be information that is unavailable or not immediately available. Other forms in the Appendices are provided to augment the information in this worksheet.

THREAT WARNING INFORMATION

Date/Time threat warning discovered: _____

Name of person who discovered threat warning: _____

Type of threat warning:

☐ Security breach	☐ Witness account	☐ Phone threat
☐ Written threat	☐ Law enforcement	☐ Unusual water quality
☐ News media	☐ Consumer complaints	☐ Public health notification
☐ Other _____		

Identity of the contaminant: ☐ Known ☐ Suspected ☐ Unknown

If known or suspected, provide additional detail below

☐ Chemical ☐ Biological ☐ Radiological

Describe _____

_____

Time of contamination: ☐ Known ☐ Estimated ☐ Unknown

If known or estimated, provide additional detail below

Date and time of contamination: _____

Additional Information: _____

_____

Mode of contamination: ☐ Known ☐ Suspected ☐ Unknown

If known or suspected, provide additional detail below

Method of addition: ☐ Single dose ☐ Over time ☐ Other _____

Amount of material: _____

Additional Information: _____

_____

Site of contamination: ☐ Known ☐ Suspected ☐ Unknown
If known or suspected, provide additional detail below

Number of sites: _____
Provide the following information for each site.

Site #1
Site Name: _____

Type of facility
- ☐ Source water ☐ Treatment plant ☐ Pump station
- ☐ Ground storage tank ☐ Elevated storage tank ☐ Finished water reservoir
- ☐ Distribution main ☐ Hydrant ☐ Service connection
- ☐ Other _____

Address: _____

Additional Site Information: _____

Site #2
Site Name: _____

Type of facility
- ☐ Source water ☐ Treatment plant ☐ Pump station
- ☐ Ground storage tank ☐ Elevated storage tank ☐ Finished water reservoir
- ☐ Distribution main ☐ Hydrant ☐ Service connection
- ☐ Other _____

Address: _____

Additional Site Information: _____

Site #3
Site Name: _____

Type of facility
- ☐ Source water ☐ Treatment plant ☐ Pump station
- ☐ Ground storage tank ☐ Elevated storage tank ☐ Finished water reservoir
- ☐ Distribution main ☐ Hydrant ☐ Service connection
- ☐ Other _____

Address: _____

Additional Site Information: _____

ADDITIONAL INFORMATION

Has there been a breach of security at the suspected site? ☐ Yes ☐ No
If "Yes", review the completed 'Security Incident Report' (Appendix 8.3)

Are there any witness accounts of the suspected incident? ☐ Yes ☐ No
If "Yes", review the completed 'Witness Account Report' (Appendix 8.4)

Was the threat made verbally over the phone? ☐ Yes ☐ No
If "Yes", review the completed 'Phone Threat Report' (Appendix 8.5)

Was a written threat received? ☐ Yes ☐ No
If "Yes", review the completed 'Written Threat Report' (Appendix 8.6)

Are there unusual water quality data or consumer complaints? ☐ Yes ☐ No
If "Yes", review the completed 'Water Quality/Consumer Complaint Report' (Appendix 8.7)

Are there unusual symptoms or disease in the population? ☐ Yes ☐ No
If "Yes", review the completed 'Public Health Report' (Appendix 8.8)

Is a 'Site Characterization Report' available? ☐ Yes ☐ No
If "Yes", review the completed 'Site Characterization Report' (Module 3, Appendix 8.3)

Are results of sample analysis available? ☐ Yes ☐ No
If "Yes", review the analytical results report, including appropriate QA/QC data

Is a 'Contaminant Identification Report' available? ☐ Yes ☐ No
If "Yes", review the completed 'Sample Analysis Report' (Module 5, Appendix 8.1)

Is there relevant information available from external sources? ☐ Yes ☐ No
Check all that apply

☐ Local law enforcement	☐ FBI	☐ DW primacy agency
☐ Public health agency	☐ Hospitals / 911 call centers	☐ US EPA / Water ISAC
☐ Media reports	☐ Homeland security alerts	☐ Neighboring utilities

☐ Other _____

Point of Contact: _____

_____

Summary of key information from external sources (provide detail in attachments as necessary):

_____

_____

_____

_____

_____

_____

THREAT EVALUATION

Has normal activity been investigated as the cause of the threat warning? ☐ Yes ☐ No

Normal activities to consider

- ☐ Utility staff inspections
- ☐ Construction or maintenance
- ☐ Operational changes
- ☐ Routine water quality sampling
- ☐ Contractor activity
- ☐ Water quality changes with a known cause
- ☐ Other _____

Is the threat 'possible'? ☐ Yes ☐ No

Summarize the basis for this determination: _____

_____

_____

Response to a 'possible' threat:

- ☐ None
- ☐ Site characterization
- ☐ Isolation/containment
- ☐ Increased monitoring/security
- ☐ Other _____

Is the threat 'credible'? ☐ Yes ☐ No

Summarize the basis for this determination: _____

_____

_____

Response to a 'credible' threat:

- ☐ Sample analysis
- ☐ Site characterization
- ☐ Isolation/containment
- ☐ Partial EOC activation
- ☐ Public notification
- ☐ Provide alternate water supply
- ☐ Other _____

Has a contamination incident been confirmed? ☐ Yes ☐ No

Summarize the basis for this determination: _____

_____

_____

Response to a confirmed incident:

- ☐ Sample analysis
- ☐ Site characterization
- ☐ Isolation/containment
- ☐ Full EOC activation
- ☐ Public notification
- ☐ Provide alternate water supply
- ☐ Initiate remediation and recovery
- ☐ Other _____

How do other organizations characterize the threat?

Organization	Evaluation	Comment
☐ Local Law Enforcement	☐ Possible ☐ Credible ☐ Confirmed	
☐ FBI	☐ Possible ☐ Credible ☐ Confirmed	
☐ Public Health Agency	☐ Possible ☐ Credible ☐ Confirmed	
☐ Drinking Water Primacy Agency	☐ Possible ☐ Credible ☐ Confirmed	
☐ Other	☐ Possible ☐ Credible ☐ Confirmed	
☐ Other	☐ Possible ☐ Credible ☐ Confirmed	

SIGNOFF

Name of person responsible for threat evaluation:

Print name _____

Signature _____ Date/Time: _____

8.3 Security Incident Report Form

INSTRUCTIONS

The purpose of this form is to help organize information about a security incident, typically a security breach, which may be related to a water contamination threat. The individual who discovered the security incident, such as a security supervisor, the WUERM, or another designated individual may complete this form. This form is intended to summarize information about a security breach that may be relevant to the threat evaluation process. This form should be completed for each location where a security incident was discovered.

DISCOVERY OF SECURITY INCIDENT

Date/Time security incident discovered: _____

Name of person who discovered security incident: _____

Mode of discovery:

- ☐ Alarm (building)
- ☐ Alarm (gate/fence)
- ☐ Alarm (access hatch)
- ☐ Video surveillance
- ☐ Utility staff discovery
- ☐ Citizen discovery
- ☐ Suspect confession
- ☐ Law enforcement discovery
- ☐ Other _____

Did anyone observe the security incident as it occurred? ☐ Yes ☐ No

If "Yes", complete the 'Witness Account Report' (Appendix 8.4)

SITE DESCRIPTION

Site Name: _____

Type of facility

- ☐ Source water
- ☐ Treatment plant
- ☐ Pump station
- ☐ Ground storage tank
- ☐ Elevated storage tank
- ☐ Finished water reservoir
- ☐ Distribution main
- ☐ Hydrant
- ☐ Service connection
- ☐ Other _____

Address: _____

_____

Additional Site Information: _____

_____

BACKGROUND INFORMATION

Have the following "normal activities" been investigated as potential causes of the security incident?

- ☐ Alarms with known and harmless causes
- ☐ Utility staff inspections
- ☐ Routine water quality sampling
- ☐ Construction or maintenance
- ☐ Contractor activity
- ☐ Other _____

Was this site recently visited *prior* to the security incident? ☐ Yes ☐ No
If "Yes," provide additional detail below

Date and time of previous visit: _____

Name of individual who visited the site: _____

Additional Information: _____
_____

Has *this location* been the site of previous security incidents? ☐ Yes ☐ No
If "Yes," provide additional detail below

Date and time of most recent security incident: _____

Description of incident: _____
_____
_____

What were the results of the threat evaluation for this incident?
☐ 'Possible' ☐ 'Credible' ☐ 'Confirmed'

Have security incidents occurred at *other locations* recently? ☐ Yes ☐ No
If "Yes", complete additional 'Security Incident Reports' (Appendix 8.3) for each site

Name of 1st additional site: _____
Name of 2nd additional site: _____
Name of 3rd additional site: _____

SECURITY INCIDENT DETAILS

Was there an alarm(s) associated with the security incident? ☐ Yes ☐ No
If "Yes," provide additional detail below

Are there sequential alarms (e.g., alarm on a gate and a hatch)? ☐ Yes ☐ No

Date and time of alarm(s): _____

Describe alarm(s): _____
_____

Is video surveillance available from the site of the security incident? ☐ Yes ☐ No
If "Yes," provide additional detail below

Date and time of video surveillance: _____

Describe surveillance: _____
_____
_____
_____

Unusual equipment found at the site and time of discovery of the security incident:

- ☐ Discarded PPE (e.g., gloves, masks)
- ☐ Tools (e.g., wrenches, bolt cutters)
- ☐ Lab equipment (e.g., beakers, tubing)
- ☐ None
- ☐ Empty containers (e.g., bottles, drums)
- ☐ Hardware (e.g., valves, pipe)
- ☐ Pumps or hoses
- ☐ Other _____

Describe equipment: _____

Unusual vehicles found at the site and time of discovery of the security incident:

- ☐ Car/sedan
- ☐ SUV
- ☐ Pickup truck
- ☐ Flatbed truck
- ☐ Construction vehicle
- ☐ None
- ☐ Other _____

Describe vehicles (including make/model/year/color, license plate #, and logos or markings): ____

Signs of tampering at the site and time of discovery of the security incident:

- ☐ Cut locks/fences
- ☐ Open/damaged access hatches
- ☐ Facility in disarray
- ☐ Open/damaged gates, doors, or windows
- ☐ Missing/damaged equipment
- ☐ None
- ☐ Other _____

Are there signs of sequential intrusion (e.g., locks removed from a gate and hatch)? ☐ Yes ☐ No

Describe signs of tampering: _____

Signs of hazard at the site and time of discovery of the security incident:

- ☐ Unexplained or unusual odors
- ☐ Unexplained dead or stressed vegetation
- ☐ Unexplained clouds or vapors
- ☐ Unexplained dead animals
- ☐ Unexplained liquids
- ☐ None
- ☐ Other _____

Describe signs of hazard: _____

SIGNOFF

Name of person responsible for documenting the security incident:

Print name _____

Signature _____ Date/Time: _____

8.4 Witness Account Report Form

INSTRUCTIONS

The purpose of this form is to document the observations of a witness to activities that might be considered an incident warning. The individual interviewing the witness, or potentially the witness, should complete this form. This may be the WUERM or an individual designated by incident command to perform the interview. If law enforcement is conducting the interview (which may often be the case), then this form may serve as a prompt for "utility relevant information" that should be pursued during the interview. This form is intended to consolidate the details of the witness account that may be relevant to the threat evaluation process. This form should be completed for each witness that is interviewed.

BASIC INFORMATION

Date/Time of interview: _____

Name of person interviewing the witness: _____

Witness contact information

Full Name: _____
Address: _____
Day-time phone: _____
Evening phone: _____
E-mail address: _____

Reason the witness was in the vicinity of the suspicious activity: _____
_____
_____

WITNESS ACCOUNT

Date/Time of activity: _____

Location of activity:

Site Name: _____

Type of facility

☐ Source water	☐ Treatment plant	☐ Pump station
☐ Ground storage tank	☐ Elevated storage tank	☐ Finished water reservoir
☐ Distribution main	☐ Hydrant	☐ Service connection
☐ Other _____		

Address: _____
_____

Additional Site Information: _____
_____

Type of activity

☐ Trespassing ☐ Vandalism ☐ Breaking and entering
☐ Theft ☐ Tampering ☐ Surveillance
☐ Other _____

Additional description of the activity _____

Description of suspects

Were suspects present at the site? ☐ Yes ☐ No

How many suspects were present? _____

Describe each suspect's appearance:

Suspect #	Sex	Race	Hair color	Clothing	Voice
1					
2					
3					
4					
5					
6					

Where any of the suspects wearing uniforms? ☐ Yes ☐ No
If "Yes," describe the uniform(s): _____

Describe any other unusual characteristics of the suspects: _____

Did any of the suspects notice the witness? ☐ Yes ☐ No
If "Yes," how did they respond: _____

Vehicles at the site

Were vehicles present at the site? ☐ Yes ☐ No

Did the vehicles appear to belong to the suspects? ☐ Yes ☐ No

How many vehicles were present? _____

Describe each vehicle:

Vehicle #	Type	Color	Make	Model	License plate
1					
2					
3					
4					
5					
6					

Where there any logos or distinguishing markings on the vehicles? ☐ Yes ☐ No
If "Yes," describe: _____

Provide any additional detail about the vehicles and how they were used (if at all): _____

Equipment at the site

Was any unusual equipment present at the site? ☐ Yes ☐ No

☐ Explosive or incendiary devices
☐ PPE (e.g., gloves, masks)
☐ Tools (e.g., wrenches, bolt cutters)
☐ Lab equipment (e.g., beakers, tubing)
☐ Other _____
☐ Firearms
☐ Containers (e.g., bottles, drums)
☐ Hardware (e.g., valves, pipe, hoses)
☐ Pumps and related equipment

Describe the equipment and how it was being used by the suspects (if at all): _____

Unusual conditions at the site

Were there any unusual conditions at the site? ☐ Yes ☐ No

☐ Explosions or fires
☐ Dead/stressed vegetation
☐ Other _____
☐ Fogs or vapors
☐ Dead animals
☐ Unusual odors
☐ Unusual noises

Describe the site conditions: _____

Additional observations

Describe any additional details from the witness account: _____

_____

_____

_____

_____

_____

SIGNOFF

Name of interviewer:

Print name _____

Signature _____ Date/Time: _____

Name of witness:

Print name _____

Signature _____ Date/Time: _____

8.5 Phone Threat Report Form

INSTRUCTIONS

This form is intended to be used by utility staff that regularly answer phone calls from the public (e.g., call center operators). The purpose of this form is to help these staff capturer as much information from a threatening phone call while the caller is on the line. It is important that the operator keep the caller on the line as long as possible in order to collect additional information. Since this form will be used during the call, it is important that operators become familiar with the content of the form. The sections of the form are organized with the information that should be collected during the call at the front of the form (i.e., Basic Call Information and Details of Threat) and information that can be completed immediately following the call at the end of the form (i.e., the description of the caller). The information collected on this form will be critical to the threat evaluation process.

Remember, tampering with a drinking water system is a crime under the SDWA Amendments!

THREAT NOTIFICATION

Name of person receiving the call: _____

Date phone call received: _____ **Time phone call received:** _____

Time phone call ended: _____ **Duration of phone call:** _____

Originating number: _____ **Originating name:** _____

*If the number/name is not displayed on the caller ID, press *57 (or call trace) at the end of the call and inform law enforcement that the phone company may have trace information.*

Is the connection clear? ☐ Yes ☐ No

Could call be from a wireless phone? ☐ Yes ☐ No

DETAILS OF THREAT

Has the water already been contaminated? ☐ Yes ☐ No

Date and time of contaminant introduction known? ☐ Yes ☐ No

Date and time if known: _____

Location of contaminant introduction known? ☐ Yes ☐ No

Site Name: _____

Type of facility

☐ Source water	☐ Treatment plant	☐ Pump station
☐ Ground storage tank	☐ Elevated storage tank	☐ Finished water reservoir
☐ Distribution main	☐ Hydrant	☐ Service connection
☐ Other _____		

Address: _____

_____

Additional Site Information: _____

_____

Name or type of contaminant known? ☐ Yes ☐ No

Type of contaminant

☐ Chemical ☐ Biological ☐ Radiological

Specific contaminant name/description: _____

_____

Mode of contaminant introduction known? ☐ Yes ☐ No

Method of addition: ☐ Single dose ☐ Over time ☐ Other _____

Amount of material: _____

Additional Information: _____

_____

Motive for contamination known? ☐ Yes ☐ No

☐ Retaliation/revenge ☐ Political cause ☐ Religious doctrine

☐ Other _____

Describe motivation: _____

_____

CALLER INFORMATION

Basic Information:

Stated name: _____

Affiliation: _____

Phone number: _____

Location/address: _____

Caller's Voice:

Did the voice sound disguised or altered? ☐ Yes ☐ No

Did the call sound like a recording? ☐ Yes ☐ No

Did the voice sound? ☐ Male / ☐ Female ☐ Young / ☐ Old

Did the voice sound familiar? ☐ Yes ☐ No

If 'Yes,' who did it sound like? _____

Did the caller have an accent? ☐ Yes ☐ No

If 'Yes,' what nationality? _____

How did the caller sound or speak?

☐ Educated ☐ Well spoken ☐ Illiterate

☐ Irrational ☐ Obscene ☐ Incoherent

☐ Reading a script ☐ Other _____

What was the caller's tone of voice?

☐ Calm	☐ Angry	☐ Lisping	☐ Stuttering/broken
☐ Excited	☐ Nervous	☐ Sincere	☐ Insincere
☐ Slow	☐ Rapid	☐ Normal	☐ Slurred
☐ Soft	☐ Loud	☐ Nasal	☐ Clearing throat
☐ Laughing	☐ Crying	☐ Clear	☐ Deep breathing
☐ Deep	☐ High	☐ Raspy	☐ Cracking

☐ Other _____

Were there background noises coming from the caller's end?

☐ Silence		
☐ Voices	describe	_____
☐ Children	describe	_____
☐ Animals	describe	_____
☐ Factory sounds	describe	_____
☐ Office sounds	describe	_____
☐ Music	describe	_____
☐ Traffic/street sounds	describe	_____
☐ Airplanes	describe	_____
☐ Trains	describe	_____
☐ Ships or large boats	describe	_____

☐ Other: _____

SIGNOFF

Name of call recipient:

Print name _____

Signature _____ Date/Time: _____

Name of person completing form (if different from call recipient):

Print name _____

Signature _____ Date/Time: _____

8.6 Written Threat Report Form

INSTRUCTIONS

The purpose of this form is to summarize significant information from a written threat received by a drinking water utility. This form should be completed by the WUERM or an individual designated by incident command to evaluate the written threat. The summary information provided in this form is intended to support the threat evaluation process; however, the completed form is not a substitute for the complete written threat, which may contain additional, significant details.

The written threat itself (e.g., the note, letter, e-mail message, etc.) may be considered evidence and thus should be minimally handled (or not handled at all) and placed into a clean plastic bag to preserve any forensic evidence.

Remember, tampering with a drinking water system is a crime under the SDWA Amendments!

SAFETY

A suspicious letter or package could pose a threat in and of itself, so caution should be exercised if such packages are received. The US Postal Service has issued guidance when dealing with suspicious packages (http://www.usps.com/news/2001/press/pr01_1022gsa.htm).

THREAT NOTIFICATION

Name of person receiving the written threat: _____

Person(s) to whom threat was addressed: _____

Date threat received: _____ **Time threat received:** _____

How was the written threat received?

☐ US Postal service ☐ Delivery service ☐ Courier
☐ Fax ☐ E-mail ☐ Hand delivered
☐ Other _____

If mailed, is the return address listed? ☐ Yes ☐ No

_____

_____

If mailed, what is the date and location of the postmark? _____

_____

If delivered, what was the service used (list any tracking numbers)? _____

_____

If Faxed, what is the number of the sending fax? _____

If E-mailed, what is the e-mail address of sender? _____

_____

If hand-delivered, who delivered the message? _____

_____

DETAILS OF THREAT

Has the water already been contaminated? ☐ Yes ☐ No

Date and time of contaminant introduction known? ☐ Yes ☐ No

Date and time if known: _____

Location of contaminant introduction known? ☐ Yes ☐ No

Site Name: _____

Type of facility

☐ Source water ☐ Treatment plant ☐ Pump station
☐ Ground storage tank ☐ Elevated storage tank ☐ Finished water reservoir
☐ Distribution main ☐ Hydrant ☐ Service connection
☐ Other _____

Address: _____

_____

Additional Site Information: _____

_____

Name or type of contaminant known? ☐ Yes ☐ No

Type of contaminant

☐ Chemical ☐ Biological ☐ Radiological

Specific contaminant name/description: _____

_____

Mode of contaminant introduction known? ☐ Yes ☐ No

Method of addition: ☐ Single dose ☐ Over time ☐ Other _____

Amount of material: _____

Additional Information: _____

_____

Motive for contamination known? ☐ Yes ☐ No

☐ Retaliation/revenge ☐ Political cause ☐ Religious doctrine
☐ Other _____

Describe motivation: _____

_____

NOTE CHARACTERISITCS

Perpetrator Information:

Stated name: _____
Affiliation: _____
Phone number: _____
Location/address: _____

Condition of paper/envelop:

☐ Marked personal ☐ Marked confidential ☐ Properly addressed
☐ Neatly typed or written ☐ Clean ☐ Corrected or marked-up
☐ Crumpled or wadded up ☐ Soiled/stained ☐ Torn/tattered
☐ Other: _____

How was the note prepared?

☐ Handwritten in print ☐ Handwritten in script ☐ Computer typed
☐ Machine typed ☐ Spliced (e.g., from other typed material)
☐ Other: _____

If handwritten, does writing look familiar? ☐ Yes ☐ No

_____

Language:

☐ Clear English ☐ Poor English
☐ Another language: _____
☐ Mixed languages: _____

Writing Style

☐ Educated ☐ Proper grammar ☐ Logical
☐ Uneducated ☐ Poor grammar/spelling ☐ Incoherent
☐ Use of slang ☐ Obscene
☐ Other: _____

Writing Tone

☐ Clear ☐ Direct ☐ Sincere
☐ Condescending ☐ Accusatory ☐ Angry
☐ Agitated ☐ Nervous ☐ Irrational
☐ Other: _____

SIGNOFF

Name of individual who received the threat:

Print name _____

Signature _____ Date/Time: _____

Name of person completing form (if different from written threat recipient):

Print name _____

Signature _____ Date/Time: _____

8.7 Water Quality/Consumer Complaint Report Form

INSTRUCTIONS

This form is provided to guide the individual responsible for evaluating unusual water quality data or consumer complaints. It is designed to prompt the analyst to consider various factors or information when evaluating the unusual data. The actual data used in this analysis should be compiled separately and appended to this form. The form can be used to support the threat evaluation due to a threat warning from unusual water quality or consumer complaints, or another type of threat warning in which water quality data or consumer complaints are used to support the evaluation.

Note that in this form, water quality refers to both specific water quality parameters and the general aesthetic characteristics of the water that might result in consumer complaints.

Threat warning is based on: ☐ Water quality ☐ Consumer complaints ☐ Other

What is the water quality parameter or complaint under consideration?

Are unusual consumer complaints corroborated by unusual water quality data?

Is the unusual water quality indicative of a particular contaminant of concern? For example, is the color, order, or taste associated with a particular contaminant?

Are consumers in the affected area experiencing any unusual health symptoms?

What is 'typical' for consumer complaints for the current season and water quality?

Number of complaints.
Nature of complaints.
Clustering of complaints

What is considered to be 'normal' water quality (i.e., what is the baseline water quality data or level of consumer complaints)?

What is reliability of the method or instrumentation used for the water quality analysis?

Are standards and reagents OK?
Is the method/instrument functioning properly?

Based on recent data, does the unusual water quality appear to be part of a gradual trend (i.e., occurring over several days or longer)?

Are the unusual water quality observations sporadic over a wide area, or are they clustered in a particular area?

What is the extent of the area? A pressure zone. A neighborhood. A city block. A street. A building.

If the unusual condition isolated to a specific area:

Is this area being supplied by a particular plant or source water?
Have there been any operational changes at the plant or in the affected area of the system?
Has there been any flushing or distribution system maintenance in the affected area?
Has there been any repair or construction in the area that could impact water quality?

SIGNOFF

Name of person completing form:

Print name _____

Signature _____ Date/Time: _____

8.8 Public Health Information Report Form

INSTRUCTIONS

The purpose of this form is to summarize significant information about a public health episode that could be linked to contaminated water. This form should be completed by the WUERM or an individual designated by incident command. The information compiled in this form is intended to support the threat evaluation process.

In the case of a threat warning due to a report from public health, it is likely that the public health agency will assume incident command during the investigation. The drinking water utility will likely play a support role during the investigation, specifically to help determine whether or not water might be the cause.

PUBLIC HEALTH NOTIFICATION

Date and Time of notification: _____ _____

Name of person who received the notification: _____

Contact information for individual providing the notification

Full Name: _____
Title: _____
Organization: _____
Address: _____
Day-time phone: _____
Evening phone: _____
Fax Number: _____
E-mail address: _____

Why is this person contacting the drinking water utility? _____
_____
_____

Has the state or local public health agency been notified? ☐ Yes ☐ No

If "No," the appropriate public health official should be immediately notified.

DESCRIPTION OF PUBLIC HEALTH EPISODE

Nature of public health episode:

☐ Unusual disease (mild) ☐ Unusual disease (severe) ☐ Death
☐ Other: _____

Symptoms:

☐ Diarrhea ☐ Vomiting/nausea ☐ Flu-like symptoms
☐ Fever ☐ Headache ☐ Breathing difficulty
☐ Other: _____

Describe symptoms: _____
_____

Causative Agent: ☐ Known ☐ Suspected ☐ Unknown

If known or suspected, provide additional detail below

☐ Chemical ☐ Biological ☐ Radiological

Describe _____

Estimate of time between exposure and onset of symptoms: _____

Exposed Individuals:

Location where exposure is thought to have occurred

☐ Residence ☐ Work ☐ School
☐ Restaurant ☐ Shopping mall ☐ Social gathering
☐ Other: _____

Additional notes on location of exposure: _____

Collect addresses for specific locations where exposure is thought to have occurred.

Is the pattern of exposure clustered in a specific area? ☐ Yes ☐ No

Extent of area

☐ Single building ☐ Complex (several buildings) ☐ City block
☐ Neighborhood ☐ Cluster of neighborhoods ☐ Large section of city
☐ Other: _____

Additional notes on extent of area: _____

Do the exposed individuals represent a disproportionate number of:

☐ Immune compromised ☐ Elderly ☐ Children
☐ Infants ☐ Pregnant women ☐ Women
☐ Other: _____
☐ None, no specific groups dominate the makeup of exposed individuals

EVALUATION OF LINK TO WATER

Are the symptoms consistent with typical waterborne diseases, such as gastrointestinal disease, vomiting, or diarrhea? ☐ Yes ☐ No

Does the area of exposure coincide with a specific area of the system, such as a pressure zone or area feed by a specific plant? ☐ Yes ☐ No

Were there any consumer complaints within the affected area? ☐ Yes ☐ No

Were there any unusual water quality data within the affected area? ☐ Yes ☐ No

Were there any process upsets or operational changes? ☐ Yes ☐ No

Was there any construction/maintenance within the affected area? ☐ Yes ☐ No

Were there any security incidents within the affected area? ☐ Yes ☐ No

SIGNOFF

Name of person completing form:

Print name _____

Signature _____ Date/Time: _____

8.9 Overview of the "Water Contaminant Information Tool"

What is the WCIT? Fundamentally, the Water Contaminant Information Tool (WCIT) is a compilation of information on nontraditional water contaminants. Nontraditional contaminants are those that are not significant from a regulatory or operational perspective, but which could have substantial adverse consequences to the public and/or utility if accidentally or intentionally introduced into the drinking water. The WCIT contains peer-reviewed information about these nontraditional contaminants that is relevant to the drinking water treatment industry. This information is managed in a relational database that will allow a user to search and sort contaminant information based on key properties. It will also allow users to create summary reports for each contaminant.

What is the purpose of the WCIT? This tool is being developed to support the drinking water treatment industry in the management of water contamination threats and incidents. It will provide relevant, accurate information to users for a variety of non-traditional drinking water contaminants. This information will be relevant to planning for and responding to drinking water contamination threats and incidents. As a planning tool, the WCIT can be used to support vulnerability assessments, emergency response plans, and the development of site-specific response guidelines. As a response tool, the WCIT can provide information about specific water contaminants, which will be necessary to make appropriate response decisions. (The WCIT will likely be **most** useful as a response tool.)

What type of information will be contained in the WCIT? The nontraditional contaminants in the WCIT will include pathogens, chemicals, and radionuclides that are of concern to drinking water. For each contaminant, the following type of information will be included in the WCIT, when available:

- Contaminant properties, such as solubility, volatility, and thermal stability.
- Fate and transport information that indicates the persistence of the contaminant in water.
- Toxicity data for chemicals and infectivity data for pathogens.
- Signs and symptoms of exposure to the contaminant.
- Efficacy of treatment processes for removing or neutralizing the contaminant.
- Methods to detect the contaminant.
- Impact of the contaminant on environmental indicators.

What is the Status of the WCIT? The WCIT is currently under development. A system prototype has been designed, constructed and populated with an initial set of data for testing. The results of system testing will be used to refine the design and functionality of the system. Next, the system will be fully populated with information for priority contaminants. It is anticipated that an initial version of the WCIT will be made available in late 2004.

Office of Ground Water and Drinking Water
Water Security Division
EPA 817-D-03-002
www.epa.gov/safewater/security
December 2003

Recycled/Recyclable • Printed with Vegetable Oil Based Inks on
100% Postconsumer, Process Chlorine Free Recycled Paper